

Dominion® KX II

KX2-116	KX2-216	KX2-416
KX2-132	KX2-232	KX2-432
		KX2-464



User Guide Release 2.0.1

Copyright © 2007 Raritan, Inc.

DKX2-0D-E

June 2007

255-62-4023-00

This page intentionally left blank.

Copyright and Trademark Information

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without the express prior written consent of Raritan, Inc.

© Copyright 2007 Raritan, Inc., CommandCenter®, RaritanConsole, Dominion®, and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer and Active Directory are registered trademarks of Microsoft® Corporation. Netscape® and Netscape Navigator are registered trademarks of Netscape Communication Corporation. All other marks are registered trademarks or trademarks of their respective manufacturers.

© Copyright 2007 GoAhead Software, Inc. All Rights Reserved.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.



For assistance in North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (refer to [Appendix A: Specifications](#) for additional information).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Contents

Chapter 1: Introduction	1
Dominion KX II Overview	1
Virtual Media	2
Product Photos.....	3
Product Features.....	4
Hardware	4
Software	4
Terminology	5
Package Contents.....	5
User Guide	6
Overview.....	6
Organization of Information	6
Related Documentation	6
Chapter 2: Getting Started	7
Login Information	7
Default IP Address	7
Supported Operating Systems (Clients)	7
Supported Browsers.....	7
Supported Operating Systems and CIMs (Target Servers).....	8
Chapter 3: Installation and Configuration	9
Overview	9
Step 1: Configure Target Servers	9
Video Resolution.....	9
Desktop Background	10
Mouse Settings.....	10
Operating System Mouse and Video Settings	10
Step 2 (Optional): Configure Keyboard Language.....	18
Step 3: Configure Network Firewall Settings	18
Step 4: Connect the Equipment	19
Step 5: Dominion KX II Initial Configuration.....	21
Changing the Default Password	21
Assigning an IP Address.....	22
Naming Target Servers.....	23
Specifying Power Supply Auto-detection	23
Note to CC-SG Users	24
Remote Authentication.....	25
Supported Protocols	25
Authentication vs. Authorization	26
Users, Groups, and Access Permissions.....	27
Overview.....	27
Users	27
Groups.....	27
Relationship between Users and Groups	27
Chapter 4: Connecting to the Dominion KX II	29
User Interfaces.....	29
KX II Local Console – KX II Devices.....	29
KX II Remote Console – KX II Devices.....	29
Multi-Platform Client (MPC) – KX I and KX II Devices	30
Raritan Remote Client (RRC) – KX I Devices Only.....	30
Language Support.....	31
Java® Runtime Environment (JRE)	31
Launching the KX II.....	32
KX II Console Layout.....	33
KX II Console Navigation.....	34
Logging Out	34
KX II Console Menu Tree	35
Managing Favorites.....	36
Manage Favorites Menu	37
Favorites List	38

Discover Devices – Local Subnet	40
Discover Devices – KX Subnet.....	41
Add New Favorite	42
Chapter 5: Accessing Target Servers	43
Port Access Page.....	43
Port Action Menu.....	44
Connecting to a Target Server.....	45
Switching between Target Servers	45
Disconnecting Target Servers.....	45
Power Controlling a Target Server.....	46
Power Cycle a Target Server.....	46
Power On a Target Server.....	46
Power Off a Target Server.....	46
Chapter 6: Virtual KVM Client	47
Note to CC-SG Users	47
Options	48
Menu Tree	48
Toolbar	48
Mouse Pointer Synchronization	49
Connection Menu	51
Properties Dialog	51
Connection Info.....	53
Exit.....	53
Keyboard Menu	54
Send Ctrl+Alt+Delete	54
Keyboard Macros.....	54
Video Menu	57
Refresh Screen.....	57
Auto-sense Video Settings	57
Calibrate Color.....	57
Video Settings	58
Mouse Menu	60
Synchronize Mouse	60
Single Mouse Cursor	60
Standard	61
Intelligent	61
Absolute.....	61
Virtual Media	61
Tools Menu	62
Options	62
View Menu	63
View Toolbar.....	63
Scaling.....	63
Target Screen Resolution	63
Help Menu.....	63
About Raritan Virtual KVM Client.....	63
Chapter 7: Virtual Media	65
Overview	65
Prerequisites for Using Virtual Media.....	66
Using Virtual Media.....	66
Opening a KVM Session	67
Connecting to Virtual Media.....	67
Local Drives.....	67
CD-ROM/DVD-ROM/ISO Images	68
Disconnecting Virtual Media	69
File Server Setup (File Server ISO Images Only).....	70
Chapter 8: User Management.....	71
User List	72
Add New User	73
Modify Existing User	74
User Group List	75
Add New User Group.....	76

Setting Permissions	77
Setting Port Permissions	77
Group-based IP ACL (Access Control List)	78
Modify Existing User Group	80
Change Password.....	82
Authentication Settings	83
Implementing LDAP Remote Authentication.....	85
Implementing RADIUS Remote Authentication	87
Chapter 9: Device Management	89
Network Settings	90
Network Basic Settings.....	91
Network Miscellaneous Settings.....	92
LAN Interface Settings.....	92
Date/Time Settings.....	94
Event Management.....	95
Event Management – Settings.....	95
Event Management – Destinations	97
SNMP Agent Configuration.....	98
SNMP Trap Configuration.....	99
Power Supply Setup Page	100
Port Configuration Page.....	101
Power Control	102
Connect the Power Strip.....	102
Name the Power Strip (Port Page for Power Strips)	103
Associate Target Servers to Outlets (Port Page)	104
Chapter 10: Security Settings	107
Security Settings	108
Login Limitations.....	109
Strong Passwords.....	109
User Blocking	110
Encryption & Share.....	111
IP Access Control.....	113
Chapter 11: Maintenance	115
Audit Log	116
Device Information	117
Backup and Restore.....	118
CIM Upgrade.....	120
Firmware Upgrade	121
Upgrade Report.....	123
Reboot.....	124
Chapter 12: Diagnostics	125
Diagnostics Menu.....	125
Network Interface Page.....	126
Network Statistics Page	127
Ping Host Page	129
Trace Route to Host Page	130
KX Diagnostics.....	131
Chapter 13: KX II Local Console	133
KX II Local Console.....	133
Physical Connections	133
Reset Button.....	134
Starting the KX II Local Console	135
KX II Local Console Interface	135
Accessing Target Servers	136
Local Port Administration	138
Local Port Settings (KX II Local Console Only)	138
Factory Reset (KX II Local Console Only)	140
Chapter 14: CC Unmanage	141
Overview	141

Removing Dominion KX II from CC-SG Management	141
Appendix A: Specifications	143
Remote Connection	144
KVM Properties	144
TCP and UDP Ports Used	145
Target Server Connection Distance and Video Resolution	146
Network Speed Settings.....	146
Appendix B: Updating the LDAP Schema	147
Returning User Group Information	147
From LDAP	147
From Microsoft Active Directory	147
Setting the Registry to Permit Write Operations to the Schema	147
Creating a New Attribute	147
Adding Attributes to the Class	148
Updating the Schema Cache	149
Editing RCI User Group Attributes for User Members	149
Appendix C: Informational Notes	151
Overview	151
Non-US Keyboards	151
French Keyboard	151
Java Runtime Environment (JRE).....	152
Keyboard Language Preference (Fedora Linux Clients).....	152
Macintosh Keyboard	152
Mouse Pointer Synchronization (Fedora)	153
Resolving Fedora Core Focus	153
SUSE/VESA Video Modes.....	153
CIMs	154
Windows 3-Button Mouse on Linux Targets	154
Virtual Media	154
Dell OptiPlex and Dimension Computers.....	154
Virtual Media not Refreshed after Files Added	154
Target BIOS Boot Time with Virtual Media	154
CC-SG.....	154
Virtual KVM Client Version not Known from CC-SG Proxy Mode	154
Proxy Mode and MPC.....	154
Appendix D: FAQs	155
General Questions	155
Remote Access	157
Universal Virtual Media	159
Ethernet and IP Networking	160
Servers	163
Installation	164
Local Port	166
Power Control	168
Scalability	169
Computer Interface Modules (CIMs).....	170
Security	171
Manageability	172
Miscellaneous	173
Troubleshooting	174

Figures

Figure 1: Dominion KX II Configuration.....	1
Figure 2: Dominion KX2-116.....	3
Figure 3: Dominion KX2-432.....	3
Figure 4: Dominion KX II CIMs: D2CIM-VUSB (left); D2CIM-PWR (right).....	3
Figure 5: Terminology and Topology	5
Figure 6: Solaris Mouse Configuration.....	15
Figure 7: Dominion KX II Connections	19
Figure 8: Network Settings.....	22
Figure 9: Port Configuration	23
Figure 10: Authentication/Authorization Flow Diagram	26
Figure 11: Dominion KX II Remote Console Login Page	32
Figure 12: KX II Remote Console Main Page	33
Figure 13: KX II Local Console Main Page	33
Figure 14: Sample Menu Hierarchy (breadcrumbs)	34
Figure 15: KX II Console Menu Tree (Local and Remote)	35
Figure 16: Favorite Devices (sidebar)	36
Figure 17: Manage Favorites Menu	37
Figure 18: Favorites List	38
Figure 19: Edit (Favorite Information)	39
Figure 20: Discover Devices - Local Subnet	40
Figure 21: Discover Devices – KX Subnet	41
Figure 22: Add New Favorite	42
Figure 23: Port Access.....	43
Figure 24: Port Action Menu	45
Figure 25: Port Action Menu (power options).....	46
Figure 26: Virtual KVM Client Window	47
Figure 27: Virtual KVM Client Menu Tree	48
Figure 28: Dual Mouse Cursors	49
Figure 29: Properties Dialog	51
Figure 30: Connection Info.....	53
Figure 31: Keyboard Macros.....	54
Figure 32: Add Keyboard Macro	55
Figure 33: Keyboard Macro Example.....	55
Figure 34: New Macro in Keyboard Menu.....	56
Figure 35: Video Settings.....	58
Figure 36: Single Mouse Cursor Message	60
Figure 37: (Tools) Options	62
Figure 38: Virtual Media Connection.....	65
Figure 39: Open KVM Session.....	67
Figure 40: Map Virtual Media Drive.....	67
Figure 41: Map Virtual Media CD/ISO Image.....	68

Figure 42: File Server Setup	70
Figure 43: User Management Menu	71
Figure 44: User List.....	72
Figure 45: User Page.....	73
Figure 46: User Group List.....	75
Figure 47: Group Page	76
Figure 48: Group-based IP Access Control List.....	78
Figure 49: IP ACL Example.....	79
Figure 50: Modify Group	80
Figure 51: Change Password.....	82
Figure 52: Authentication Settings	83
Figure 53: Authentication Settings (LDAP).....	85
Figure 54: Authentication Settings (RADIUS)	87
Figure 55: Device Settings Menu	89
Figure 56: Network Settings.....	90
Figure 57: Network Settings (Network Basic Settings).....	91
Figure 58: Network Settings (Network Miscellaneous Settings).....	92
Figure 59: Network Settings (LAN Interface Settings).....	92
Figure 60: Date/Time Settings	94
Figure 61: Event Management – Settings.....	95
Figure 62: Syslog Configuration.....	96
Figure 63: Event Management - Destinations.....	97
Figure 64: Power Supply Setup	100
Figure 65: Port Configuration.....	101
Figure 66: Power Strip Connections	102
Figure 67: Port Page (power strips)	103
Figure 68: Port Page (KVM ports).....	104
Figure 69: Port Page (Target Server Settings for D2CIM-VUSB).....	105
Figure 70: Security Menu	107
Figure 71: Security Settings.....	108
Figure 72: Security Settings (Strong Passwords).....	109
Figure 73: Security Settings (User Blocking).....	110
Figure 74: Security Settings (Encryption & Share).....	111
Figure 75: Security Settings (Encryption Mode Warning Message).....	111
Figure 76: IP Access Control	113
Figure 77: Maintenance Menu	115
Figure 78: Audit Log.....	116
Figure 79: Device Information	117
Figure 80: Backup/Restore	118
Figure 81: CIM Upgrade from KX Flash.....	120
Figure 82: Firmware Upgrade	121
Figure 83: Firmware Upgrade Review	122
Figure 84: Firmware Upgrade Successful.....	122

Figure 85: Upgrade Report	123
Figure 86: Reboot	124
Figure 87: Reboot Confirmation	124
Figure 88: Diagnostics Menu	125
Figure 89: Network Interface	126
Figure 90: Network Statistics (statistics)	127
Figure 91: Network Statistics (interfaces)	127
Figure 92: Network Statistics (route)	128
Figure 93: Ping Host	129
Figure 94: Trace Route to Host	130
Figure 95: KX Diagnostics	131
Figure 96: Diagnostics Scripts	132
Figure 97: File Download	132
Figure 98: Dominion KX II Local Console	133
Figure 99: Local User Panel on Dominion KX II	133
Figure 100: Reset Button (back of unit)	134
Figure 101: Local Console Port Access	136
Figure 102: Local Port Settings	138
Figure 103: Factory Reset (Local Console Only)	140
Figure 104: Device Managed by CC-SG Message	141
Figure 105: Remove from CC-SG Management	141
Figure 106: Confirm CC Unmanage	142
Figure 107: Device Removed from CC Management	142
Figure 108: Create New Attribute	148
Figure 109: Adding the Attributes to the Class	148
Figure 110: ADSI Edit	149
Figure 111: User Properties	150
Figure 112: Edit Attribute (adding user to KX II group)	150

Chapter 1: Introduction

Dominion KX II Overview

Dominion KX II is an enterprise-class, secure, digital KVM (Keyboard, Video, Mouse) switch that provides BIOS-level (and up) access, and control of up to 64 servers from anywhere in the world via Web browser. At the rack, Dominion KX II provides BIOS-level control of up to 64 servers and other IT devices from a single keyboard, monitor, and mouse. The integrated remote access capabilities of the Dominion KX II provide the same levels of control of your servers via Web browser.

Dominion KX II is easily installed using standard UTP (Cat 5/5e/6) cabling. Its advanced features include virtual media, 128-bit encryption, dual power supplies, remote power control, dual Ethernet, LDAP, RADIUS, Active Directory, Syslog integration, and Web management. These features enable you to deliver higher uptime, better productivity, and bulletproof security – at any time from anywhere.

Dominion KX II products can operate as standalone appliances and do not rely on a central management device. For larger data centers and enterprises, numerous Dominion KX II units (along with Dominion SX units for remote serial console access and Dominion KSX for remote/branch office management) can be integrated into a *single* logical solution using Raritan's CommandCenter Secure Gateway (CC-SG) management appliance.

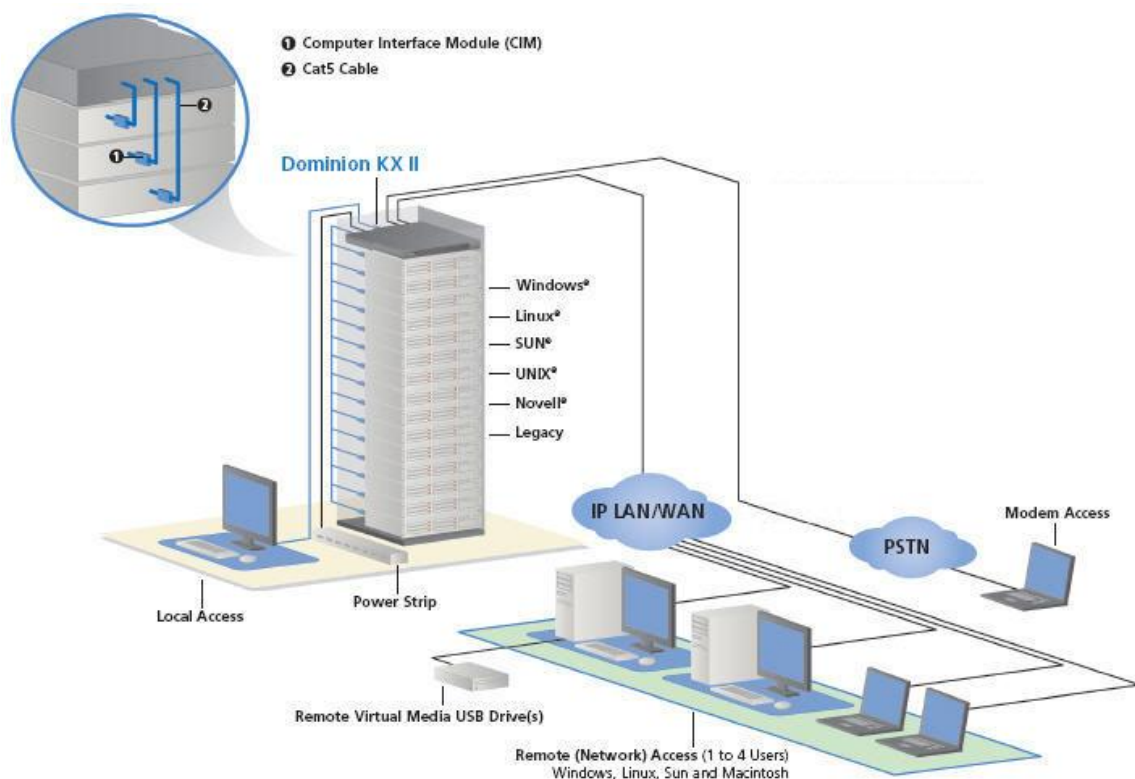


Figure 1: Dominion KX II Configuration

Virtual Media

All Dominion KX II models support virtual media. The benefits of virtual media – mounting of remote drives/media on the target server to support software installation, and diagnostics – are now available in all of the Dominion KX II models.

Each Dominion KX II comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, internal and remote drives and images. Unlike other solutions, the Dominion KX II supports virtual media access of hard drives and remotely mounted images for added flexibility and productivity.

Virtual media sessions are secured using 128-bit AES or RC4 encryption.

The new D2CIM-VUSB CIM (computer interface module) supports virtual media sessions to target servers supporting the USB 2.0 interface. This new CIM also supports Absolute Mouse Synchronization™ as well as remote firmware update.

Product Photos



Figure 2: Dominion KX2-116



Figure 3: Dominion KX2-432



Figure 4: Dominion KX II CIMs: D2CIM-VUSB (left); D2CIM-PWR (right)

Product Features

Hardware

- Integrated KVM-over-IP remote access
- 1U or 2U (KX2-464) rack-mountable; brackets included
- Dual power supplies with failover; auto-switching power supply with power failure warning
- 16, 32, or 64 (on KX2-464) server ports
- Multiple user capacity (1/2/4 remote users; 1 local user)
- UTP (Cat5/5e/6) server cabling
- Dual Ethernet ports (10/100/1000 LAN) with failover
- Field upgradeable
- Local user port for in-rack access
 - PS/2 keyboard/mouse ports
 - One front and three back panel USB 2.0 ports for supported USB devices
 - Fully concurrent with remote user access
 - Local Graphical User Interface (GUI) for administration
- Centralized access security
- Integrated power control
- LED indicators for dual power status, network activity, and remote user status
- Hardware reset button

Software

- Virtual media with D2CIM-VUSB CIM
- Absolute Mouse Synchronization with D2CIM-VUSB CIM
- Plug-and-Play
- Web-based access and management
- Intuitive Graphical User Interface (GUI)
- 128-bit encryption of complete KVM signal, including video and virtual media
- LDAP, Active Directory, RADIUS, or internal authentication and authorization
- DHCP or fixed IP addressing
- SNMP and Syslog management
- Power control associated directly with servers to prevent mistakes
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management appliance
- CC Unmanage feature to remove device from CC-SG control

Terminology

This manual uses the following terminology for the components of a typical Dominion KX II configuration:

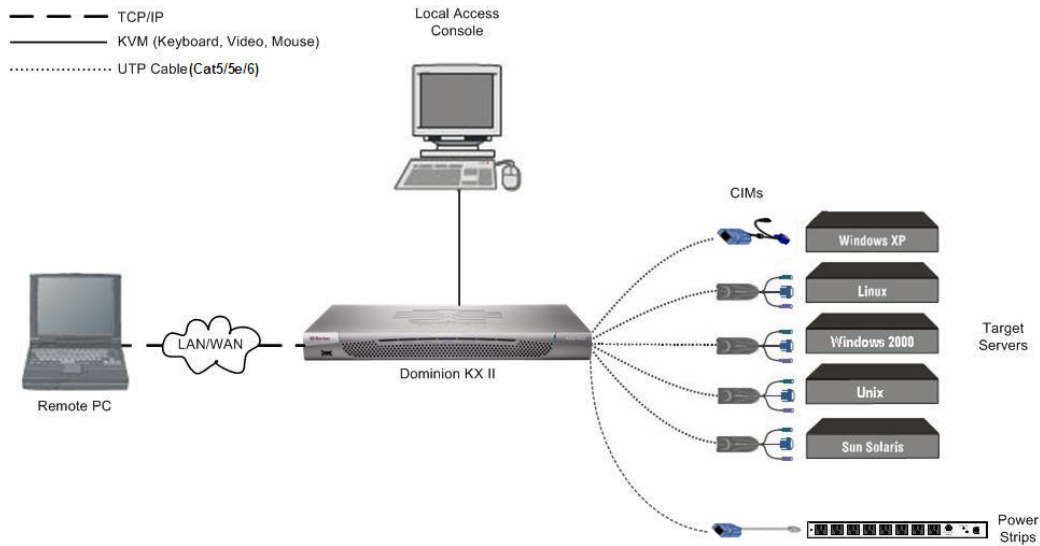


Figure 5: Terminology and Topology

**Remote PC
(client)**

Networked computers used to access and control target servers connected to the Dominion KX II. Refer to [Supported Operating Systems \(Clients\)](#) for a list of the Operating Systems supported by Dominion KX II remotely.

**Local Access Console
(client)**

An optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to Dominion KX II to control target servers locally (directly at the rack, not through the network).

**CIMs
(Computer Interface Modules)**

Dongles that connect to each target server and Raritan power strip. Available for all of the supported Operating Systems. Refer to [Supported CIMs](#) for information about the CIMs supported by Dominion KX II.

Target Servers

Servers with video cards and user interfaces (e.g., Windows®, Linux®, Solaris™, etc.) accessed remotely via Dominion KX II. Refer to [Supported Operating Systems and CIMs \(Target Servers\)](#) for a list of the supported Operating Systems and CIMs.

Power Strips

Raritan power strips accessed remotely via the Dominion KX II.

Package Contents

Each Dominion KX II ships as a fully-configured stand-alone product in a standard 1U (2U for KX2-464) 19" rackmount chassis. Each Dominion KX II unit ships with the following contents:

- (1) Dominion KX II Unit
- (1) Dominion KX II Quick Installation and Setup Guide
- (1) Raritan User Manuals CD-ROM
- (1) Rackmount Kit
- (2) AC Power Cords
- (1) Cat5 Network Cable
- (1) Cat5 Network Crossover Cable
- (1) Set of 4 Rubber Feet (for desktop use)
- (1) Application Note
- (1) Warranty Card

User Guide

Overview

The Dominion KX II User Guide provides the information to install, set up and configure, access target servers and power strips, use virtual media, manage users and security, and maintain and diagnose the Dominion KX II.

This user guide is specific to Dominion KX II (version 2.0); for information pertaining to version 1.4, refer to the *Dominion KX 1.4 User Guide*.

Organization of Information

The user guide is organized as follows:

- Chapter 1, *Introduction*. Overview, features, terminology, and package contents
- Chapter 2, *Getting Started*. Login information; default IP Address; supported operating systems, browsers, and CIMs
- Chapter 3, *Installation and Configuration*. Target server configuration; firewall settings; physical device connections; initial KX II unit configuration; remote authentication; and users, groups, and access permissions
- Chapter 4, *Connecting to the Dominion KX II*. User interfaces; starting the KX II Remote Console; Dominion KX II Favorites
- Chapter 5, *Accessing Target Servers*. Access, control, and switching between target servers
- Chapter 6, *Virtual KVM Client*. Target server control, mouse pointer synchronization, keyboard macros, and video settings
- Chapter 7, *Virtual Media*. Virtual media configuration and access
- Chapter 8, *User Management*. User and group management, passwords, group-based IP access control, and authentication settings
- Chapter 9, *Device Management*. Network settings, date/time, event management, power supply setup, port configuration, and power control
- Chapter 10, *Security Settings*. Security settings and IP access control
- Chapter 11, *Maintenance*. Audit log; device information; backup and restore; firmware and CIM upgrades; and reboot
- Chapter 12, *Diagnostics*. Network interface, network statistics, ping host, trace route to host, and KX diagnostics
- Chapter 13, *KX II Local Console*. Starting the KX II Local Console, accessing target servers, and local port administration
- Chapter 14, *CC Unmanage*. Removing the KX II from CC-SG control
- Appendix A, *Specifications*. Physical specifications; ports used; target server connection distance and video resolution; and network speed settings
- Appendix B, *Updating the LDAP Schema*. Update LDAP schema (for experienced users)
- Appendix C, *Informational Notes*. Important notes on Dominion KX II usage
- Appendix D, *FAQs*. General questions, remote access, universal virtual media, Ethernet and IP networking, servers, installation, local port, power control, scalability, Computer Interface Modules (CIMs), security, manageability, miscellaneous, and troubleshooting

Related Documentation

For more information about the Raritan Multi-Platform Client (MPC), refer to the *Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide*.

For more information about the entire Raritan product line, refer to the *Raritan User Manuals & Quick Setup Guides CD ROM* or Raritan's Web site

<http://www.raritan.com/support/productdocumentation>

Chapter 2: Getting Started

Login Information

- The default Dominion KX II login user name is **admin** and the default password is **raritan**. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password **raritan** must be entered entirely in lowercase letters.
- The first time you start the Dominion KX II you are required to change the default password.

Tip: For backup and business continuity purposes, it is strongly recommended that you create a backup administrator user name and password and keep that information in a secure location.

Default IP Address

Dominion KX II ships with the default IP address of 192.168.0.192.

Supported Operating Systems (Clients)

The following operating systems are supported on the Dominion KX II Remote Console, Virtual KVM Client™, and Multi-Platform Client (MPC):

CLIENT OS	VIRTUAL MEDIA (VM) SUPPORT ON CLIENT
Windows XP	Yes
Windows 2000 SP4	Yes
Windows Vista	Yes
Red Hat Linux 9.0	Yes; Locally held ISO image, Remote File Server mounting directly from KX
Red Hat Enterprise Workstation 3.0 and 4.0	Yes; Locally held ISO image, Remote File Server mounting directly from KX
SUSE Linux Professional 9.2 and 10	Yes; Locally held ISO image, Remote File Server mounting directly from KX
Fedora™ Core 5 and above	Yes; Locally held ISO image, Remote File Server mounting directly from KX
Mac®	No
Solaris	No

Supported Browsers

Dominion KX II supports the following browsers:

- Internet Explorer 6 and 7
- Firefox® 1.5 and 2.0
- Mozilla® 1.7
- Safari 2.0

Supported Operating Systems and CIMs (Target Servers)

In addition to the new Dominion KX II D2CIMs, most Paragon® and Dominion KX I CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes:

TARGET SERVER	SUPPORTED CIMs			VM	MOUSE MODES		
	PARAGON CIMs	DOMINION KX I DCIMs	DOMINION KX II D2CIMs		AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server Windows 2003 Server Windows Vista	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓	✓	✓
Red Hat Linux 9.0 Red Hat Enterprise Workstation 3.0 and 4.0	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (excluding Red Hat Enterprise Workstation 3.0)	✓			✓
SUSE Linux Professional 9.2 and 10	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora Core 3 and above	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
All Solaris OSs supported in Dominion KX I	P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB DCIM-USB G2					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Remote Power Strips			D2CIM-PWR				
Serial Devices	P2CIM-SER						

Legend:

- VM: Virtual Media (D2CIM-VUSB only)
- AM: Absolute Mouse Synchronization (D2CIM-VUSB only)
- IM: Intelligent Mouse Mode
- SM: Standard Mouse Mode
- ✓: Supported

Note: D2CIM-VUSB is not supported on Sun (Solaris) targets.

Chapter 3: Installation and Configuration

Overview

This section provides a brief overview of the installation process. Each step is further detailed in the remaining sections of this chapter.

To install and configure Dominion KX II:

1. Configure the target servers.
2. (Optional) Configure the keyboard language.
3. Configure the network firewall settings.
4. Connect the equipment.
5. Configure the Dominion KX II unit.

Step 1: Configure Target Servers

Target servers are the computers that will be accessed and controlled via the Dominion KX II. Before installing Dominion KX II, configure *all* target servers to ensure optimum performance. This configuration applies only to *target servers*, not to the client workstations (remote PCs) used to access Dominion KX II remotely. Refer to [Chapter 1: Introduction, Terminology](#) for additional information.

To configure the target servers:

- Check the video resolution.
- Check the desktop background.
- Adjust the mouse settings.
- Perform OS-specific mouse and video configuration.

Video Resolution

Ensure that each target server's video resolution and refresh rate are supported by Dominion KX II and that the signal is *non-interlaced*.

Supported Video Resolutions

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. Refer to [Target Server Connection Distance and Video Resolution](#) for more information. Dominion KX II supports these resolutions:

640x350 @70 Hz	720x400 @85 Hz	1024x768 @90 Hz
640x350 @85 Hz	800x600 @56 Hz	1024x768 @100 Hz
640x400 @56 Hz	800x600 @60 Hz	1152x864 @60 Hz
640x400 @84 Hz	800x600 @70 Hz	1152x864 @70 Hz
640x400 @85 Hz	800x600 @72 Hz	1152x864 @75 Hz
640x480 @60 Hz	800x600 @75 Hz	1152x864 @85 Hz
640x480 @66.6 Hz	800x600 @85 Hz	1152x870 @75.1 Hz
640x480 @72 Hz	800x600 @90 Hz	1152x900 @66 Hz
640x480 @75 Hz	800x600 @100 Hz	1152x900 @76 Hz
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz
640x480 @90 Hz	1024x768 @60 Hz	1280x960 @85 Hz
640x480 @100 Hz	1024x768 @70 Hz	1280x1024 @60 Hz
640x480 @120 Hz	1024x768 @72 Hz	1280x1024 @75 Hz
720x400 @70 Hz	1024x768 @75 Hz	1280x1024 @85 Hz
720x400 @84 Hz	1024x768 @85 Hz	1600x1200 @60 Hz

Note: Composite Sync and Sync-on-Green video require an additional adapter.

Desktop Background

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces such as Windows, Linux, X-Windows, Solaris, and KDE require configuration. The desktop background need not be *completely* solid; but desktop backgrounds featuring photos or complex gradients might degrade performance.

Mouse Settings

The Dominion KX II operates in several mouse modes:

- [Absolute Mouse Synchronization](#) (D2CIM-VUSB only)
- [Intelligent Mouse Mode](#) (do not use an animated mouse)
- [Standard Mouse Mode](#)

For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described later in this manual. Mouse parameters do not have to be altered for Absolute Mouse Synchronization; D2CIM-VUSB is required for this mode. Mouse configurations will vary on different target operating systems; consult your OS documentation for additional detail.

Intelligent mouse mode generally works well on most Windows platforms. Intelligent mouse mode may produce unpredictable results when active desktop is set on the target. For additional information on Intelligent Mouse mode, refer to the *Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization)* available on Raritan's Website

<http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion KX II shipment.

Operating System Mouse and Video Settings

This section provides video mode and mouse information specific to the Operating System in use on the target server.

Windows XP / Windows 2003 Settings

[To configure target servers running Microsoft Windows XP/2003:](#)

1. Configure the mouse settings:
 - a. Select **Start > Control Panel > Mouse**.
 - b. Open the **Pointer Options** tab. In the **Motion** group:
 - Set the mouse motion speed setting exactly to the middle speed.
 - Disable the **Enhanced pointer precision** option.
 - Click **OK**.
2. Disable transition effects:
 - a. Select the **Display** option from **Control Panel**.
 - b. Open the **Appearance** tab.
 - c. Click the **Effects** button.
 - d. Clear the **Use the following transition effect for menus and tooltips** option.
 - e. Click **OK**.
 - f. Close the Control Panel.

Note: For target servers running Windows 2000 or XP, you may wish to create a user name that will be used only for remote connections through Dominion KX II. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the Dominion KX II connection.

Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal Dominion KX II performance. As a result, mouse synchronization may not be optimal for these screens. **WARNING!** Proceed only if you are comfortable adjusting the registry on Windows target servers. You can obtain better Dominion KX II mouse synchronization at login screens by using the Windows registry editor to change the following settings (HKEY_CURRENT_USER\Control Panel\Mouse): MouseSpeed = 0; MouseThreshold 1 = 0; MouseThreshold 2 = 0.

Windows 2000 Settings

To configure target servers running Microsoft Windows 2000:

1. Configure the mouse settings:
 - a. Select **Start > Control Panel > Mouse**.
 - b. Open the **Motion** tab.
 - Set the acceleration to **None**.
 - Set the mouse motion speed setting exactly to the middle speed.
 - Click **OK**.
2. Disable transition effects:
 - a. Select the **Display** option from **Control Panel**.
 - b. Open the **Effects** tab.
 - c. Clear the **Use the following transition effect for menus and tooltips** option.
 - d. Click **OK**.
 - e. Close the Control Panel.

Windows Vista

To configure target servers running Microsoft Windows Vista:

1. Configure the mouse settings:
 - a. Select **Start > Settings > Control Panel > Mouse**.
 - b. Open the **Pointer Options** tab. In the **Motion** group:
 - Set the mouse motion speed setting exactly to the middle speed.
 - Disable the **Enhanced pointer precision** option.
 - Click **OK**.
2. Disable animation and fade effects:
 - a. Select the **System** option from **Control Panel**.
 - b. Select **Advanced system settings**. The System Properties dialog opens.
 - c. Open the **Advanced** tab.
 - d. Click the **Settings** button in the Performance group. The Performance Options dialog opens.
 - e. Under **Custom** options, clear the following checkboxes:

<i>Animation options:</i>	
	Animate controls and elements inside windows
	Animate windows when minimizing and maximizing
<i>Fade options:</i>	
	Fade or slide menus into view
	Fade or slide ToolTips into view
	Fade out menu items after clicking

- f. Click **OK**.
- g. Close the Control Panel.

Linux Settings (Red Hat 9)

***Note:** The following settings are optimized for standard mouse mode only.*

To configure target servers running Linux (graphical user interface):

1. Configure the mouse settings:
 - a. Select **Main Menu > Preferences > Mouse**. The Mouse Preferences dialog opens.
 - b. Open the **Motion** tab.
 - c. Within the **Speed** group, set the **Acceleration** slider to the exact center.
 - d. Within the **Speed** group, set the **Sensitivity** towards low.
 - e. Within the **Drag & Drop** group, set the **Threshold** towards small.
 - f. Close the Mouse Preferences dialog.

***Note:** If these steps do not work, issue the **xset mouse 1 1** command as described in the Linux command line instructions.*

2. Configure the screen resolution:
 - a. Select **Main Menu > System Settings > Display**. The Display Settings dialog opens.
 - b. From the Display tab, select a **Resolution** supported by Dominion KX II.
 - c. From the Advanced tab, verify that the **Refresh Rate** is supported by Dominion KX II.

***Note:** Once connected to the target server, in many Linux graphical environments, the **<CTRL> <ALT> <+>** command will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.*

To configure target servers running Linux (command line):

1. Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: **xset mouse 1 1**. This should be set for execution upon login.
2. Ensure that each target server running Linux is using a resolution supported by Dominion KX II at a standard VESA resolution and refresh rate.
3. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
 - Go to the Xfree86 Configuration file XF86Config
 - Using a text editor, disable all non-Dominion KX II supported resolutions
 - Disable the virtual desktop feature (not supported by Dominion KX II)
 - Check blanking times (+/- 40% of VESA standard)
 - Restart computer

Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.

Note for Red Hat 9 Target Servers

If you are running Red Hat 9 on the target server using a USB CIM, and are experiencing problems with the keyboard and/or mouse, there is an additional configuration setting you can try.

Tip: You might have to perform these steps even after a fresh OS installation.

To configure Red Hat 9 servers using USB CIMs:

1. Locate the configuration file (usually **/etc/modules.conf**) in your system.
2. Using the editor of your choice, make sure that the **alias usb-controller** line in the **modules.conf** file is as follows:

```
alias usb-controller usb-uhci
```

Note: If there is another line using **usb-uhci** in the **/etc/modules.conf** file, it needs to be removed or commented out.

3. Save the file.
4. Reboot the system in order for the changes to take effect.

Linux Settings (Red Hat 4)

Note: The following settings are optimized for standard mouse mode only.

To configure target servers running Linux (graphical user interface):

1. Configure the mouse settings:
 - a. Select **Main Menu > Preferences > Mouse**. The Mouse Preferences dialog opens.
 - b. Open the **Motion** tab.
 - c. Within the **Speed** group, set the **Acceleration** slider to the exact center.
 - d. Within the **Speed** group, set the **Sensitivity** towards low.
 - e. Within the **Drag & Drop** group, set the **Threshold** towards small.
 - f. Close the Mouse Preferences dialog.

Note: If these steps do not work, issue the **xset mouse 1 1** command as described in the *Linux command line instructions*.

2. Configure the screen resolution:
 - a. Select **Main Menu > System Settings > Display**. The Display Settings dialog opens.
 - b. From the Settings tab, select a **Resolution** supported by Dominion KX II.
 - c. Click **OK**.

Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.

SUSE Linux 10.1 Settings

Note: Do not attempt to synchronize the mouse at the SUSE login prompt. You must be connected to the target server to synchronize the mouse cursors.

To configure the mouse settings:

1. Select **Desktop > Control Center**. The Desktop Preferences dialog opens.
2. Select **Mouse**. The Mouse Preferences dialog opens.
3. Open the **Motion** tab.
4. Within the **Speed** group, set the **Acceleration** slider to the exact center position.
5. Within the **Speed** group, set the **Sensitivity** slider to low.
6. Within the **Drag & Drop** group, set the **Threshold** slider to small.
7. Click **Close**.

To configure the video:

1. From **Desktop Preferences**, select **Graphics Card and Monitor**. The Card and Monitor Properties dialog opens.
2. Verify that a **Resolution** and **Refresh Rate** is in use that is supported by Dominion KX II. Please refer to [Supported Video Resolutions](#) for more information.

Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.

Make Linux Settings Permanent

Note: These steps may vary slightly depending on the specific version of Linux in use.

To make your settings permanent in Linux (prompt):

1. Select **Main Menu > Preferences > More Preferences > Sessions**. The Sessions dialog opens.
2. Open the **Session Options** tab.
3. Check the **Prompt on logout** checkbox and click **OK**. This option prompts you to save your current session when you logout.
4. Upon logging out, check the **Save current setup** option from the dialog presented.
5. Click **OK**.

Tip: If you do not want to be prompted upon logout, follow these procedures instead.

To make your settings permanent in Linux (no prompt):

1. Select **Main Menu > Preferences > More Preferences > Sessions**. The Session dialog opens.
2. Open the **Session Options** tab.
3. Clear the **Prompt on logout** checkbox.
4. Check the **Automatically save changes to the session** checkbox and click **OK**. This option automatically saves your current session when you logout.

Sun Solaris Settings

To configure target servers running Sun Solaris:

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed:
 - From the graphical user interface:

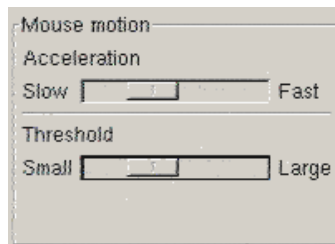


Figure 6: Solaris Mouse Configuration

- With the command line:

```
xset mouse a t
```

 (where “a” is the acceleration and “t” is the threshold.)
2. All target servers must be configured to one of the [display resolutions](#) supported by Dominion KX II. The most popular supported resolutions for Sun machines are:

DISPLAY RESOLUTION	VERTICAL REFRESH RATE	ASPECT RATIO
1600 x 1200	75 Hz	4:3
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

3. Target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync).

To change your Sun video card output from composite sync to the non-default VGA output:

1. Issue the **Stop+A** command to drop to bootprom mode.
2. Issue the following command to change the output resolution:


```
setenv output-device screen:r1024x768x70
```
3. Issue the **“boot”** command to reboot the server.

You can also contact your Raritan representative to purchase a video output adapter:

IF YOU HAVE:	USE THIS VIDEO OUTPUT ADAPTER:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

Note: Some of the standard Sun background screens may not center precisely on certain Sun servers, with dark borders. Use another background or place a light colored icon in the upper left hand corner.

Mouse Settings

To configure the mouse settings (Sun Solaris 10.1):

1. Select **Launcher**. Application Manager – Desktop Controls opens.
2. Select **Mouse Style Manager**. The **Style Manager – Mouse** dialog opens.
3. Set the **Acceleration** slider to 1.0.
4. Set the **Threshold** slider to 1.0.
5. Click **OK**.

Accessing the Command Line

1. Right click.
2. Select **Tools > Terminal**. A terminal window opens. (It is best to be at the root to issue commands.)

Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Please note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

To check current POST resolution:

Run the following command as root: **# eeprom output-device**

To change POST resolution:

1. **# eeprom output-device=screen:r1024x768x75**
2. Logout or restart computer.

Video Settings (GUI)

The GUI resolution can be checked and set using different commands depending on the video card in use. Please note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

The following table is organized by card:

CARD	TO CHECK RESOLUTION:	TO CHANGE RESOLUTION:
32-bit	# /usr/sbin/pgxconfig –prconf	<ol style="list-style-type: none"> 1. # /usr/sbin/pgxconfig –res 1024x768x75 2. Logout or restart computer.
64-bit	# /usr/sbin/m64config –prconf	<ol style="list-style-type: none"> 1. # /usr/sbin/m64config –res 1024x768x75 2. Logout or restart computer.
32-bit and 64-bit	# /usr/sbin/fbconfig –prconf	<ol style="list-style-type: none"> 1. # /usr/sbin/fbconfig –res 1024x768x75 2. Logout or restart computer.

IBM AIX 5.3 Settings

Follow these steps in this section to configure target servers running IBM AIX 5.3.

To configure the mouse:

1. Go to **Launcher**.
2. Select **Style Manager**.
3. Click **Mouse**. The Style Manager – Mouse dialog opens.
4. Use the sliders to set the **Mouse acceleration** to 1.0 and **Threshold** to 1.0.
5. Click **OK**.

To configure the video:

1. From the **Launcher**, select **Application Manager**.
2. Select **System_Admin**.
3. Select **Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate**.
4. Select the video card in use.
5. Click **List**. A list of display modes is presented.
6. Select a resolution and refresh rate supported by the Dominion KX II. Please refer to [Supported Video Resolutions](#) for more information.

Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.

Make UNIX Settings Permanent

Note: These steps may vary slightly depending on the type of UNIX (e.g., Solaris, IBM AIX) and the specific version in use.

1. Select **Style Manager > Startup**. The Style Manager – Startup dialog opens.
2. Select the **Logout Confirmation Dialog** option of **On**. This option prompts you to save your current session when you logout.

Apple Macintosh Settings

For target servers running an Apple Macintosh operating system, the preferred method is to use the D2CIM-VUSB and Absolute Mouse Synchronization.

Note: Enable the **Absolute mouse scaling for MAC server** option in the [Port](#) page.

Step 2 (Optional): Configure Keyboard Language

Note: This step is not required if you are using the US/International language keyboard.

If you are using a non-US language, the keyboard has to be configured for the appropriate language. In addition, the keyboard language for the client machine and the target servers has to match.

Please consult the documentation for your operating system for additional information about changing the keyboard layout.

Change the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and would like the keyboard layout changed to another language.

To change the keyboard layout code (DCIM-SUSB only):

1. Open a Text Editor window on the Sun workstation.
2. Check that the **NUM LOCK** key is active and press the *left* **CTRL** key and the **DEL** key on your keyboard. The **Caps Lock LED** starts to blink, indicating that the CIM is in Layout Code Change mode.
The text window displays: Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).
3. Type the layout code desired (for example, **31** for the Japanese keyboard).
4. Press **Enter**.
5. Shut down the unit and power ON once again. The DCIM-SUSB performs a reset (power cycle).
6. Using MPC, type something to verify that the characters are correct.

Step 3: Configure Network Firewall Settings

To access Dominion KX II through a network firewall, your firewall must allow communication on TCP Port 5000 or another port that you designate. Refer to [Network Settings](#) for additional information about designating another discovery port.

Firewall Settings

TO TAKE ADVANTAGE OF THE DOMINION KX II:	THE FIREWALL MUST ALLOW INBOUND COMMUNICATION ON:
Web-access capabilities	Port 443 – standard TCP port for HTTPS communication
Automatic redirection of HTTP requests to HTTPS (i.e., so users can type the more common “http://xxx.xxx.xxx.xxx” instead of “https://xxx.xxx.xxx.xxx”)	Port 80 – standard TCP port for HTTP communication

Step 4: Connect the Equipment

Connect the Dominion KX II to the power supply, network, local PC, and target servers. The numbers in the diagram correspond to the sections describing the connection.

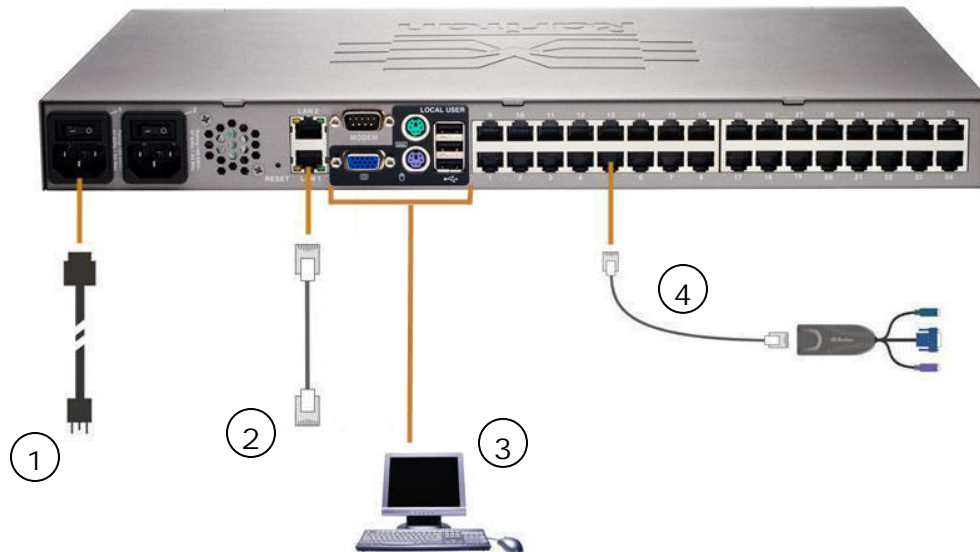


Figure 7: Dominion KX II Connections

1. AC Power

To connect the power supply:

1. Attach the included AC power cord to the Dominion KX II and plug into an AC power outlet.
2. For dual power failover protection, attach the second included AC power cord and plug it into a **different power source** than the first power cord.

Note: If you only attach one power cord, the power LED on the Dominion KX II front panel will display red because the system is set to automatically detect both sources. Refer to the [Power Supply Setup Page](#) for information about turning off automatic detection for the power source not in use.

2. Network Ports

Dominion KX II provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and the automatic failover is disabled. When enabled, if the Dominion KX II internal network interface or the network switch to which it is connected becomes unavailable, LAN2 will be enabled using the *same* IP address.

To connect the network:

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To make use of the optional Dominion KX II Ethernet failover capabilities:
 - Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.
 - **Enable Automatic Failover** on the Network Configuration screen (refer to [Network Settings, LAN Interface Settings](#) for more information).

Use both network ports only if you want to use one as a failover port.

3. Local Access Port (local PC)

For convenient access to target servers while at the rack, use the Dominion KX II Local Access port. While the local port is *required* for installation and setup, it is *optional* for subsequent use. The local port provides the KX II Local Console graphical user interface for administration and target server access.

To connect the local port:

Attach a multi-sync VGA monitor, mouse, and keyboard to the respective Local User ports (using either a PS/2 or USB keyboard and mouse).

4. Target Server Ports

Dominion KX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to [Appendix A: Specifications](#) for additional information.

To connect a target server to the Dominion KX II:

1. Use the appropriate Computer Interface Module (CIM). Refer to [Supported CIMs](#) for more information about the CIMs to use with each operating system.
2. Attach the HD15 video connector of your CIM to the video port of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.
3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your Dominion KX II unit.

Step 5: Dominion KX II Initial Configuration

The first time you power up the Dominion KX II unit, there is some initial configuration that you need to perform through the KX II Local Console:

- Change the default password.
- Assign the IP Address.
- Name the target servers.
- Specify power supply auto-detection.

Changing the Default Password

The Dominion KX II ships with a default password. *The first time you start the Dominion KX II you are required to change that password.*

To change the default password:

1. Power ON the Dominion KX II using the power switch(es) at the back of the unit. Please wait for the Dominion KX II unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the KX II Local Console is visible on the monitor attached to the Dominion KX II local port. Type the default username (**admin**) and password (**raritan**) and click **Login**. The Change Password screen is displayed.
3. Type your old password (**raritan**) in the **Old Password** field.
4. Type a new password in the **New Password** field; retype the new password in the **Confirm New Password** field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and the special characters identified in the table following these steps.
5. Click **Apply**.
6. You will receive confirmation that the password was successfully changed. Click **OK**. The Port Access page is displayed.

***Note:** The default password can also be changed from the Raritan Multi-Platform Client (MPC). For more information, refer to the **Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide**.*

Valid Special Characters

CHARACTER	DESCRIPTION	CHARACTER	DESCRIPTION
!	Exclamation point	:	Colon
"	Double quote	;	Semi-colon
#	Pound sign	=	Equal sign
\$	Dollar sign	>	Greater than sign
%	Percent sign	?	Question mark
&	Ampersand	@	At sign
'	Single quote	[Left bracket
(Left parenthesis	\	Backward slash
)	Right parenthesis]	Right bracket
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace
.	Period		Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde

Assigning an IP Address

These procedures describe how to assign an IP Address using the Network Settings page. For complete information about all of the fields and the operation of this page, refer to [Network Settings](#).

1. From the KX II Local Console, select **Device Settings > Network Settings**. The Network Settings page opens.

Figure 8: Network Settings

2. Specify a meaningful **Device Name** for your Dominion KX II unit; up to 16 alphanumeric characters, [special characters](#), and no spaces.
3. Select the **IP auto configuration** from the drop-down list:
 - **None** (Static IP). This option requires that you manually specify the network parameters. This is the recommended option because the Dominion KX II is an infrastructure device and its IP Address should not change.
 - **DHCP**. With this option, network parameters are assigned by the DHCP server.
4. If you specify an IP configuration of **None**, type the TCP/IP parameters for your Dominion KX II unit: **IP address**, **Subnet mask**, **Gateway IP address**, **Primary DNS server IP address**, and (optional) **Secondary DNS server IP address**.
5. When finished, click **OK**.

Your Dominion KX II unit is now network accessible.

Note: In some environments, the **LAN Interface Speed & Duplex** setting default of **Autodetect** (auto-negotiation) does not properly set the network parameters, resulting in network issues. In these instances, setting the Dominion KX II **LAN Interface Speed & Duplex** field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. Refer to the [Network Settings](#) page for more information.

Naming Target Servers

To name the target servers:

1. Connect all of the target servers if you have not already done so (as described in [Step 3: Connect the Equipment, Target Server Ports](#)).
2. Using the KX II Local Console, select **Device Settings > Port Configuration**. The Port Configuration page opens:

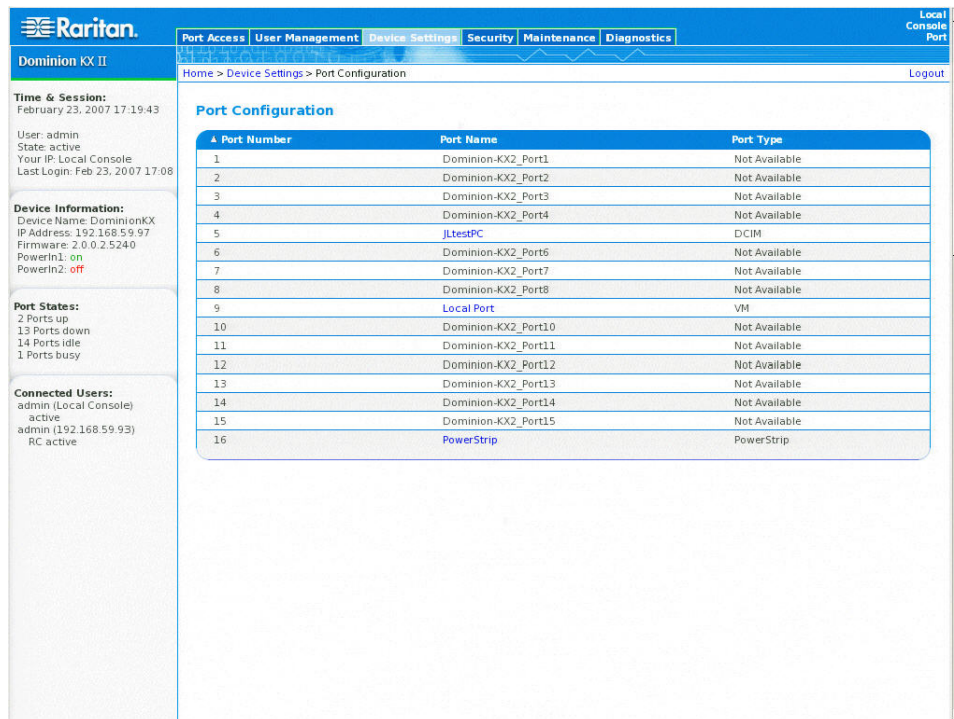


Figure 9: Port Configuration

3. Click on the **Port Name** of the target server you want to rename. The [Port Page](#) opens.
4. Assign a name to identify the server connected to that port. The name can be up to 32 characters; alphanumeric and [special characters](#) are allowed.
5. Click **OK**.

Specifying Power Supply Auto-detection

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail. The Power Supply Setup page is configured to automatically detect both power supplies; use this page to disable automatic detection of the power supply not in use.

To disable power supply auto-detection for the power supply not in use:

1. Using the KX II Local Console, select **Device Settings > Power Supply Setup**. The Power Supply Setup page opens.
2. Clear auto-detection for the power supply that you are *not* using.

For more information, refer to [Power Supply Setup Page](#).

Note to CC-SG Users

If you are using Dominion KX II in a CC-SG configuration, perform the installation steps as outlined above, and when finished, consult the *CommandCenter Secure Gateway User Guide*, *Administrator Guide*, or *Deployment Guide* to proceed (all found on Raritan's Website under Support: <http://www.raritan.com/support/productdocumentation>).

Note: *The remainder of this user guide applies primarily to deploying Dominion KX II unit(s) without the integration functionality of CC-SG.*

Remote Authentication

Note to CC-SG Users

When the Dominion KX II is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups, *except* for local users (requiring local port access). When CC-SG is controlling the KX II, local port users will be authenticated against the local user database or the Remote Authentication server (LDAP or RADIUS) configured on the KX II; they will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, refer to the *CommandCenter Secure Gateway User Guide*, *Administrator Guide*, or *Deployment Guide* at:

<http://www.raritan.com/support/productdocumentation>.

Supported Protocols

In order to simplify management of usernames and passwords, the Dominion KX II provides the capability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP and RADIUS.

Note on Microsoft Active Directory

Microsoft Active Directory uses the LDAP protocol natively, and can function as an LDAP server and authentication source for Dominion KX II. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Authentication vs. Authorization

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

When Dominion KX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

The flow diagram illustrates this process:

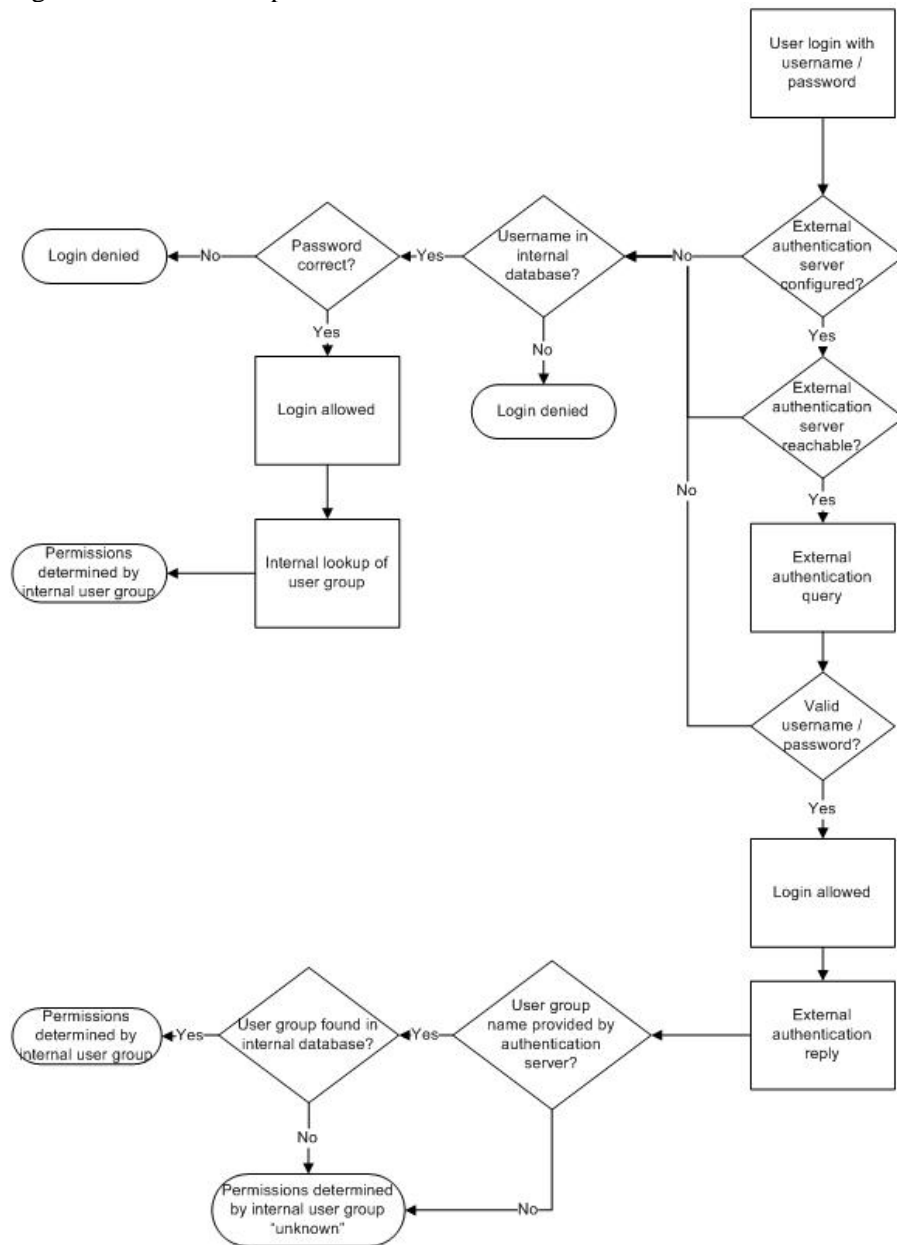


Figure 10: Authentication/Authorization Flow Diagram

Note the importance of the group to which a given user belongs, as well as the need to configure the group named, “Unknown”. If the external authentication server returns a group name that is not recognized by the Dominion KX II, that user's permissions are determined by the permanent group named “Unknown”.

Refer to [Implementing LDAP Remote Authentication](#) and [Implementing RADIUS Remote Authentication](#) to determine how to configure your authentication server to return user group information to the Dominion KX II as part of its reply to an authentication query.

Users, Groups, and Access Permissions

Overview

The Dominion KX II stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as “local authentication”. All users have to be authenticated; if Dominion KX II is configured for LDAP or RADIUS, that authentication is processed first, followed by local authentication.

Users

User names and passwords are required to gain access to the Dominion KX II unit. This information is used to authenticate users attempting to access your KX II unit. Refer to [User Management](#) for more information about adding and editing users.

Groups

Every Dominion KX II unit is delivered with three default user groups; these groups cannot be deleted:

Admin	Users that are a member of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges.
Unknown	This is the default group for users who are authenticated externally using LDAP or RADIUS. If the external LDAP or RADIUS server does not identify a valid user group, the Unknown group is used.
Individual Group	An individual group is essentially a “group” of one. That is, the specific user is in its own group, not affiliated with other <i>real</i> groups. Individual groups can be identified by the “@” in the Group Name.

In addition to the system-supplied default groups, you can create groups and specify the appropriate permissions to suit your needs. Refer to [User Management](#) for more information about creating and editing user groups.

Relationship between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your Dominion KX II into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose *not* to associate specific users with groups. In this case, you can classify the user as “Individual.”

Upon successful authentication, the device uses **Group** information to determine the user’s permissions – which server ports are accessible, whether rebooting the unit is allowed, and other features.

Chapter 4: Connecting to the Dominion KX II

User Interfaces

There are several user interfaces in the Dominion KX II providing you with easy access any time, anywhere. These include the KX II Local Console, the KX II Remote Console, and the Multi-Platform Client (MPC). The following table identifies these interfaces and their use for target server access and administration locally and remotely:

USER INTERFACE	LOCAL		REMOTE	
	ACCESS	ADMIN	ACCESS	ADMIN
KX II Local Console	✓	✓		
KX II Remote Console			✓	✓
Virtual KVM Client			✓	
Multi-Platform Client (MPC)			✓	✓

KX II Local Console – KX II Devices

When you are located at the server rack, Dominion KX II provides standard KVM switching and administration via the KX II Local Console. The KX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports.

There are many similarities among the KX II Local Console and the KX II Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The KX II Local Console and the KX II Remote Console user interfaces are almost identical; the following options are available in the KX II Local Console, but *not* the KX II Remote Console:

- [Local Port Settings](#)
- [Factory Reset](#)

KX II Remote Console – KX II Devices

The Dominion KX II Remote Console is a browser-based graphical user interface that allows you to access target servers connected to the Dominion KX II and to remotely administer the KX II.

The KX II Remote Console provides a digital connection to your connected target servers. Whenever you access a target server using the KX II Remote Console, a Virtual KVM Client window is opened. One Virtual KVM Client is opened for each target server, permitting simultaneous access when supported by the specific KX II unit (for example, KX2-116 supports only one remote session).

There are many similarities among the KX II Local Console and the KX II Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the KX II Remote Console, but *not* the KX II Local Console:

- [Virtual Media](#)
- [Favorites](#)
- [Backup/Restore](#)
- [Firmware Upgrade](#)
- [Upgrade Report](#)
- [KX Diagnostics](#)

Multi-Platform Client (MPC) – KX I and KX II Devices

The Raritan Multi-Platform Client (MPC) is a graphical interface that allows you to remotely access the target devices connected to Dominion units. MPC can be installed for standalone use or accessed through a Web browser.

After installing the Dominion KX II, either download a standalone version of Raritan MPC and establish an initial network connection, or launch the application directly.

Note: MPC supports both KX I and KX II devices; use MPC if you would like to access servers connected to both KX I and KX II devices with one user interface.

To launch MPC directly:

1. To launch MPC from a client running any browser, type **http://IP-ADDRESS/mpc** into the address line, where **IP-ADDRESS** is the IP address of your Raritan device. MPC will launch in a new window that **does not** contain a menu bar, tool bar, scroll bar, or address bar. Work in this window and toggle to other open windows using the **ALT+TAB** command.
2. When MPC launches, a device tree of all automatically detected Raritan devices found on your subnet is displayed on the left side of the screen. If you do not find your Dominion KX II unit listed by name, create an icon manually by selecting **Connection > New Profile**. The Add Connection window opens.
3. Type a device Description, specify a Connection Type, add the Dominion unit's IP Address, and click **OK**. These specifications can be edited later.
4. In the Navigator panel on the left of the screen, double-click on the icon that corresponds to your Dominion KX II unit.

Refer to the *Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide*, available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion shipment for complete information on installing and operating MPC.

Raritan Remote Client (RRC) – KX I Devices Only

Raritan Remote Client (RRC) is a graphical user interface providing remote access to the target devices.

Note: RRC *cannot* be used with the Dominion KX II; use MPC instead.

Language Support

The Dominion KX II provides keyboard support for the following languages: US English, UK English, Traditional Chinese, Simplified Chinese, Japanese, Korean, French, and German.

***Note:** You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for KX II Local Console functions.*

For more information about non-US keyboards, please refer to [Appendix C: Informational Notes](#).

Java® Runtime Environment (JRE)

Important: It is recommended that you disable Java caching and clear the Java cache. Please refer to your Java documentation or the *Raritan Multi-Platform Client (MPC)* and *Raritan Remote Client (RRC) User Guide* for more information.

The Dominion KX II Remote Console and MPC require the JRE to function. The Dominion KX II Remote Console checks the Java version; if the version is incorrect or outdated, you will be prompted to download a compatible version.

Raritan recommends using Java Runtime Environment (JRE) version 1.5 for optimum performance, but the Dominion KX II Remote Console and MPC will function with JRE version **1.4.2_05** or greater (with the exception of JRE 1.5.0_02). JRE 1.6 is also supported, but has not been fully tested.

***Note:** In order for multi-language keyboards to work in the KX II Remote Console (Virtual KVM Client) please install the multi-language version of Java Runtime Environment (JRE).*

Launching the KX II

Important: Regardless of the browser used, you must allow pop-ups from the Dominion device's IP address to launch the KX II Remote Console.

***Note:** Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the KX II Remote Console.*

You can reduce the number of warning messages in subsequent logins by checking the following options in these security and certificate warning messages:

- ☐ *In the future, do not show this warning*
 - ☐ *Always trust content from this publisher*
-

To launch the KX II Remote Console:

1. Log on to any workstation with network connectivity to your Dominion KX II unit and Java Runtime Environment v1.4.2_2 or higher installed (JRE is available at <http://java.sun.com/>).
2. Launch a [supported Web browser](#) such as Internet Explorer (IE) or Firefox.
3. Type the following URL: **http://IP-ADDRESS**, where **IP-ADDRESS** is the IP Address that you assigned to your Dominion KX II unit. You can also use **https**, the DNS name of the Dominion KX II assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP Address in the browser (KX II always redirects the IP Address from HTTP to HTTPS.) The Login page opens:

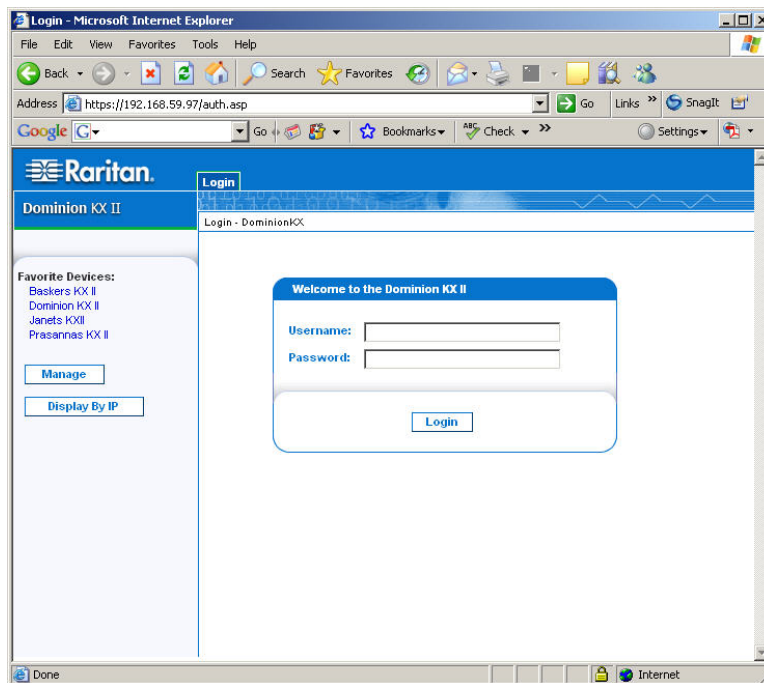


Figure 11: Dominion KX II Remote Console Login Page

4. Type your **Username** and **Password**. If this is the first time logging in, log in with the factory default username and password (**admin** and **raritan** (all lower case)); you will be prompted to change the default password. Refer to [Changing the Default Password](#) for more information.
5. Click **Login**.

KX II Console Layout

Both the KX II Remote Console and the KX II Local Console interfaces provide an HTML (Web-like) interface for configuration and administration, as well as target server list and selection. The options are organized into various tabs.

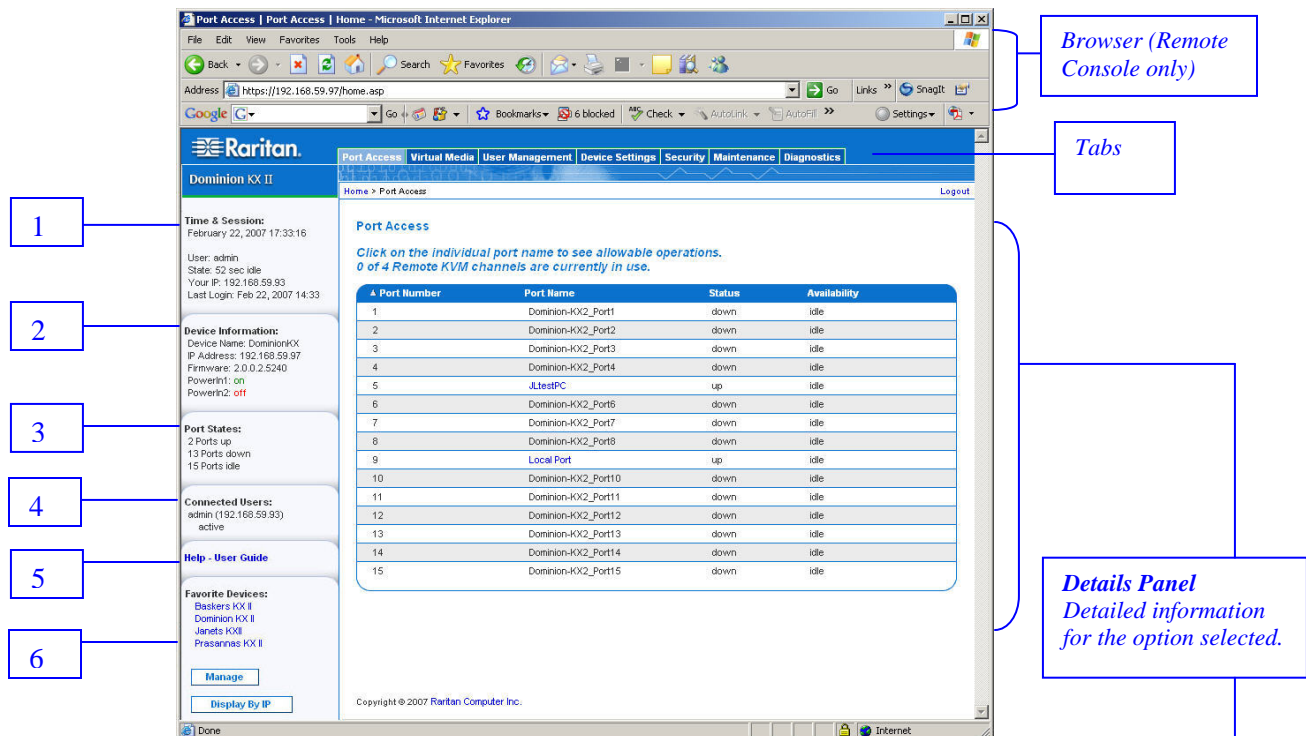


Figure 12: KX II Remote Console Main Page

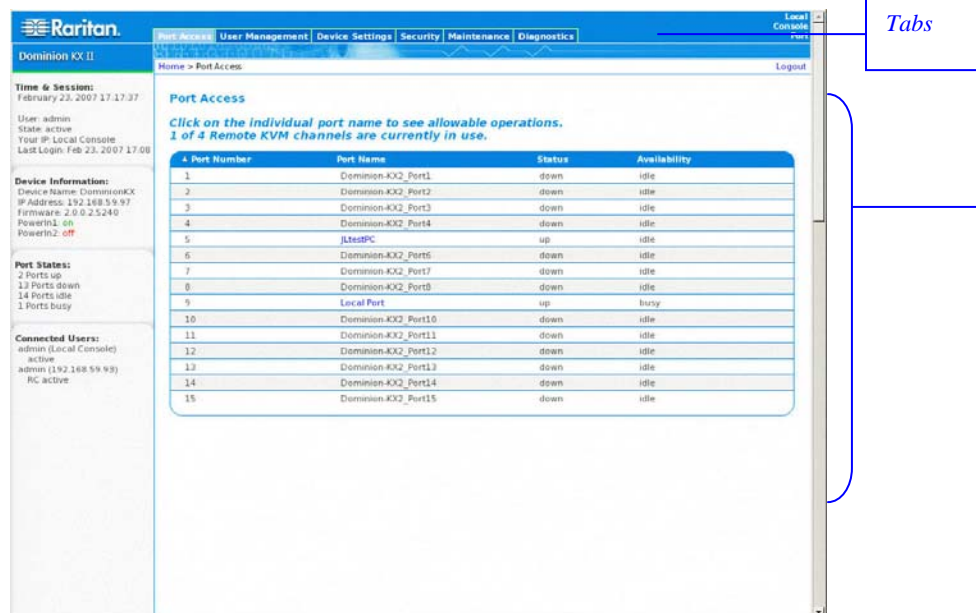


Figure 13: KX II Local Console Main Page

After successful login, the Port Access page opens listing all ports along with their status and availability. You can sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

The numbers in the following table correspond to the numbers in Figure 12.

#	TITLE	DESCRIPTION
1	Time & Session	Date, time, user name, current state, IP Address of client, and last login
2	Device Information	Device name, IP Address, firmware version, and status of both power lines
3	Port States	Current status of all Dominion KX II ports
4	Connected Users	List of all users currently connected to your Dominion KX II
5	Help – User Guide	Access to this user manual (KX II Remote Console only)
6	Favorite Devices	Access and management of your Favorites list (KX II Remote Console only)

KX II Console Navigation

The Dominion KX II Console interfaces (both local and remote) provide many methods for navigation and making your selections.

To select an option (use any of the following):

- Click on a tab; a page of available options is opened.
- Hover over a tab and select the appropriate option from the menu.
- Click the option directly from the menu hierarchy displayed (“breadcrumbs”).

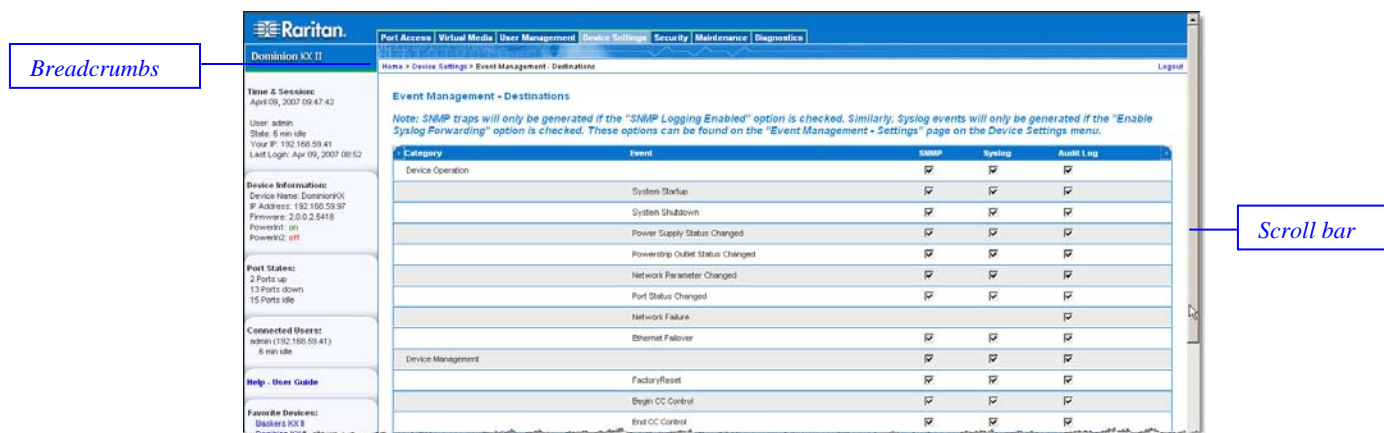


Figure 14: Sample Menu Hierarchy (breadcrumbs)

To scroll through pages longer than the screen:

- Use **Page Up** and **Page Down** keys on your keyboard, or
- Use the scroll bar on the right

For more information about navigation and selection in the Raritan Multi-Platform Client (MPC), refer to the *Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide*.

Logging Out

To quit the Dominion KX II Console:

Click **Logout** in the upper right-hand corner of the page.

Note: Logging out also closes any open Virtual KVM Client sessions.

KX II Console Menu Tree

The following diagram represents *all* of the menu options available in both the KX II Remote and KX II Local Console interfaces. Variations between the KX II Local Console and the KX II Remote Console are identified.

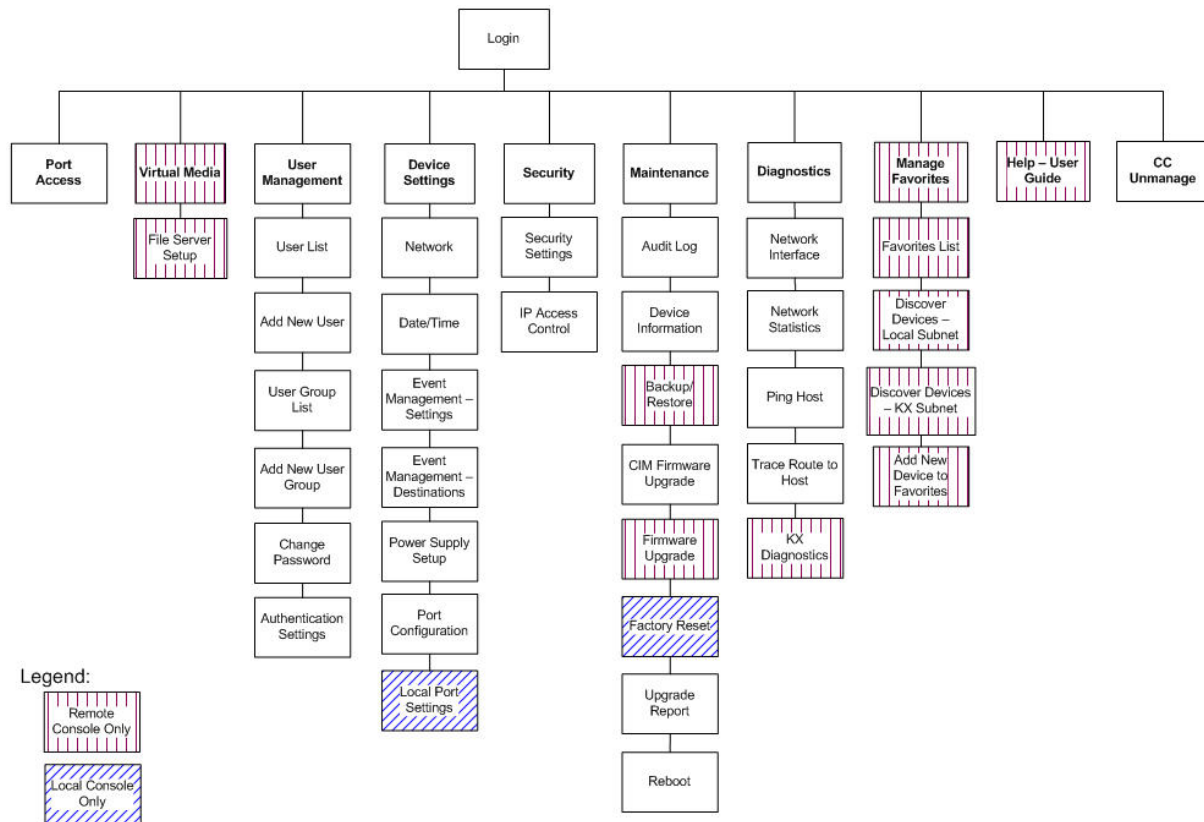


Figure 15: KX II Console Menu Tree (Local and Remote)

In addition to being identified in the menu tree above, menu option variations between the KX II Local Console and the KX II Remote Console are identified in the following table:

OPTION	LOCAL CONSOLE	REMOTE CONSOLE
Virtual Media		✓
File Server Setup		✓
Backup/Restore		✓
Firmware Upgrade		✓
KX Diagnostics		✓
Manage Favorites		✓
Favorites List		✓
Discover Devices – Local Subnet		✓
Discover Devices – KX Subnet		✓
Add New Device to Favorites		✓
Help – User Guide		✓
Local Port Settings	✓	
Factory Reset	✓	

Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently. The Favorite Devices section is located in the lower left side (sidebar) of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently used devices
- List your Favorites either by name or IP Address
- Discover Dominion KX II devices on its subnet (before and after login)
- Retrieve discovered Dominion KX II devices from the connected KX device (after login)

Note: This feature is available only on the Dominion KX II Remote Console (not the Dominion KX II Local Console).

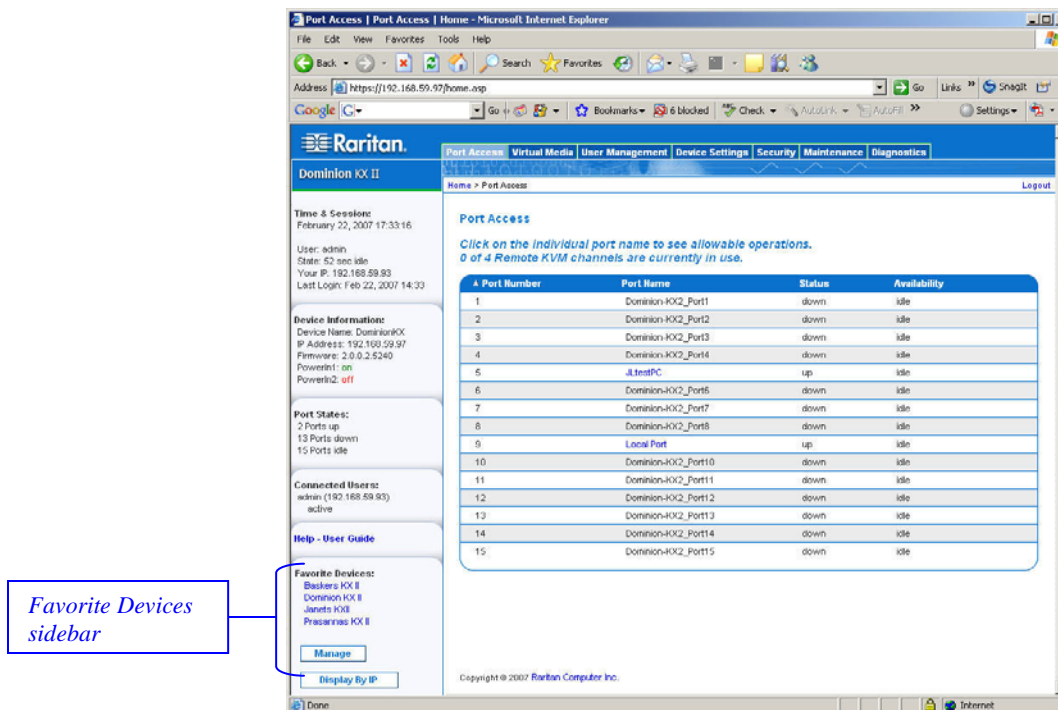


Figure 16: Favorite Devices (sidebar)

To access a favorite KX II device:

Click the device name for that device (listed beneath **Favorite Devices**). A new browser opens to that device.

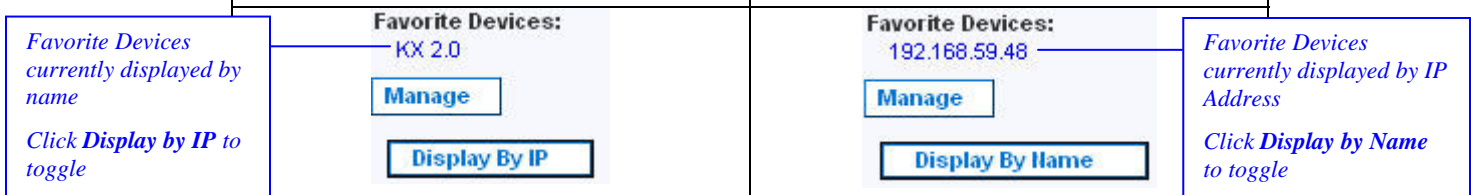
To toggle the **Favorite Devices** list display between name and IP Address:

To display Favorites by IP Address:

Click the **Display by IP** button.

To display Favorites by name:

Click the **Display by Name** button.



Manage Favorites Menu

The Manage Favorites menu provides these options: Favorites List, Discover Devices – Local Subnet, Discover Devices – KX Subnet, and Add New Device to Favorites.

To open the Manage Favorites menu:

Click the **Manage** button. The Manage Favorites page opens:

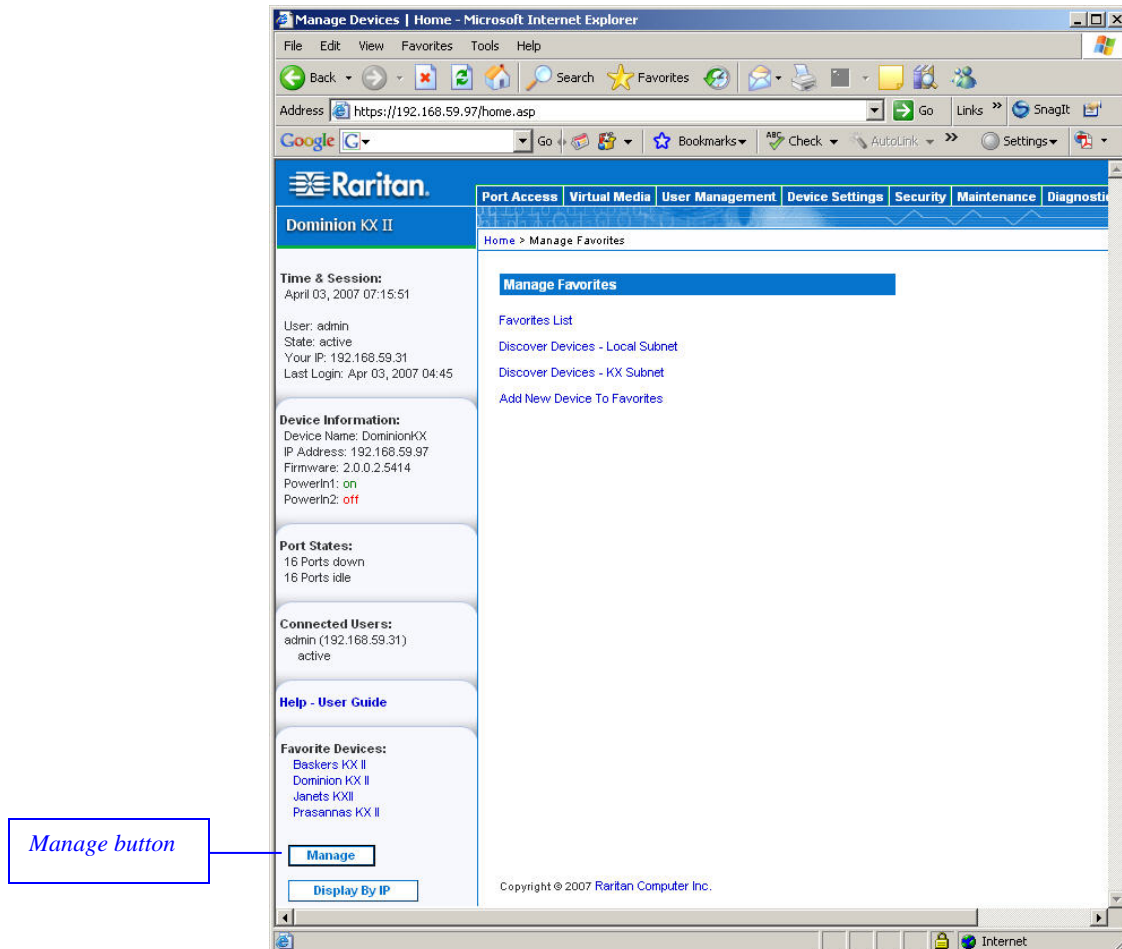


Figure 17: Manage Favorites Menu

USE:	TO:
Favorites List	Manage your list of favorite devices.
Discover Devices – Local Subnet	Discover the devices on the local subnet.
Discover Devices – KX Subnet	Discover the devices on the KX device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.

Favorites List

From the Favorites List page, you can add, edit, and delete devices from your list of Favorites.

To open the Favorites List page:

Select **Manage > Favorites List**. The Favorites List page opens:

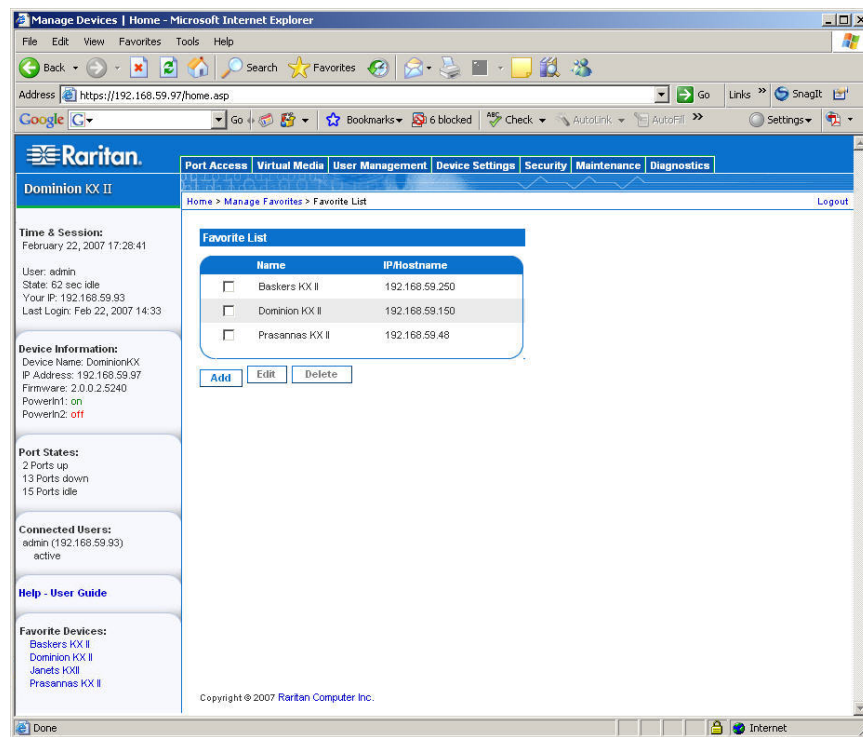


Figure 18: Favorites List

To add a Favorite:

Click the **Add** button. The [Add New Favorite](#) page opens.

To delete a Favorite:

Important: Please exercise caution in the removal of favorites; you are not prompted to confirm their deletion.

1. Check the checkbox next to the appropriate Dominion KX II device.
2. Click the **Delete** button. The favorite is removed from your list of favorites.

To edit a Favorite:

1. From the Favorites List page, check the checkbox next to the appropriate Dominion KX II device.
2. Click the **Edit** button. The Edit page opens:

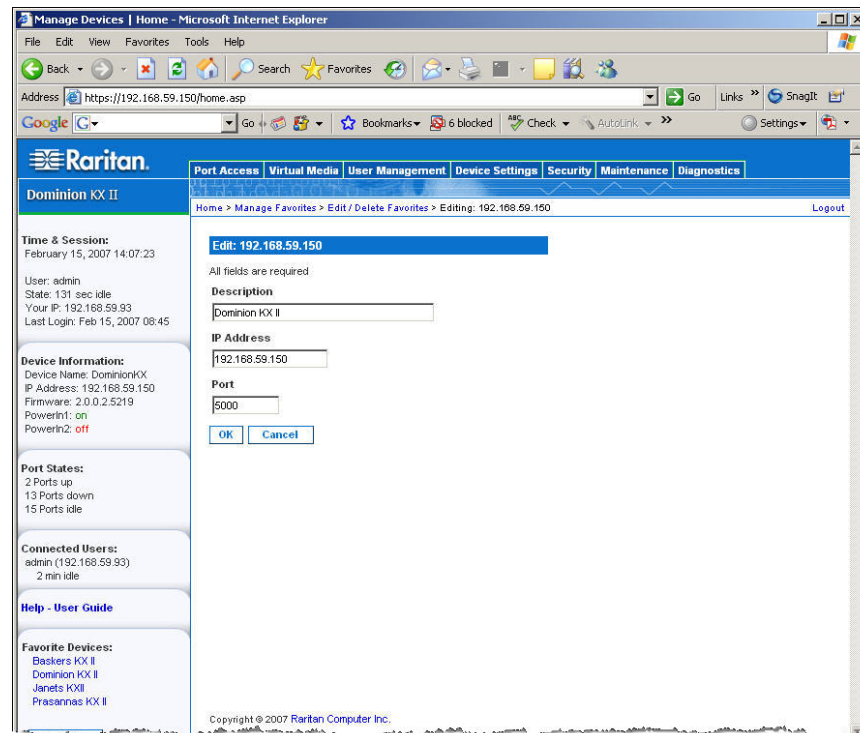


Figure 19: Edit (Favorite Information)

3. Update the fields as necessary:
 - **Description.** Type something meaningful.
 - **IP Address.** Type the IP Address of the Dominion KX II unit.
 - **Port.** Change the discovery **Port** (if necessary).
4. Click **OK**.

Discover Devices – Local Subnet

This option discovers the devices on your local subnet (that is, the subnet where the Dominion KX II Remote Console is running); access these devices directly from this page, or add them to your list of favorites.

The screenshot shows the Raritan Dominion KX II web interface. The top navigation bar includes links for Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance, and Diagnostics. The main content area is titled 'Discover Devices - Local Subnet'. It features a 'Use Default Port 5000' checkbox, a 'Discover on Port' field with the value '5000', and a 'Save' button. Below this is a table of discovered devices with columns for Name and IP/Hostname. The table lists various devices, including Annettes_KX116, Annettes_KX432, ASTDKXII-416, buntlykx, DaveKX2, Dominion-KX, DominionKX, and shivas_kx20. At the bottom of the table are buttons for 'Select All', 'Deselect All', 'Add', and 'Refresh'. The sidebar on the left contains sections for Time & Session, Device Information, Port States, Connected Users, Help - User Guide, and Favorite Devices.

Name	IP/Hostname
<input type="checkbox"/> Annettes_KX116	192.168.59.213
<input type="checkbox"/> Annettes_KX432	192.168.59.227
<input type="checkbox"/> ASTDKXII-416	192.168.59.218
<input type="checkbox"/> buntlykx	192.168.59.217
<input type="checkbox"/> DaveKX2	192.168.59.206
<input type="checkbox"/> Dominion-KX	192.168.59.240
<input type="checkbox"/> DominionKX	192.168.59.224
<input type="checkbox"/> DominionKX	192.168.59.225
<input type="checkbox"/> DominionKX	192.168.59.237
<input type="checkbox"/> DominionKX	192.168.59.239
<input type="checkbox"/> DominionKX	192.168.59.244
<input type="checkbox"/> DominionKX	192.168.59.249
<input type="checkbox"/> DominionKX	192.168.59.252
<input type="checkbox"/> DominionKX	192.168.59.253
<input type="checkbox"/> kx14	192.168.59.233
<input type="checkbox"/> kx2wrc4	192.168.59.185
<input type="checkbox"/> lraKX2	192.168.59.207
<input type="checkbox"/> shivas_kx20	192.168.59.208

Figure 20: Discover Devices - Local Subnet

To discover devices on the local subnet:

1. Select **Favorites > Discover Devices – Local Subnet**. The Discover Devices – Local Subnet page opens.
2. Select the appropriate discovery port (refer to [Network Miscellaneous Settings](#) for information about the discovery port):
 - To use the default discovery port, check the **Use Default Port 5000** option.
 - To use a different discovery port:
 - a. Clear the **Use Default Port 5000** option.
 - b. Type the port number into the **Discover on Port** field.
 - c. Click **Save**.
3. Click **Refresh**. The list of devices on the local subnet is refreshed.

To add devices to your Favorites List:

1. Check the checkbox next to the device name/IP Address.
2. Click **Add**.

*Tip: Use the **Select All** and **Deselect All** buttons to quickly select all (or deselect all) devices in the remote console subnet.*

To access a discovered device:

Click the device name or IP Address for that device. A new browser opens to that device.

Discover Devices – KX Subnet

This option discovers the devices on the KX device subnet (that is, the subnet of the Dominion KX II device IP address itself); access these devices directly from this page, or add them to your list of favorites.

This feature allows multiple Dominion KX II units to interoperate and scale automatically. The Dominion KX II Remote Console automatically discovers the Dominion KX II units in the subnet of the Dominion KX II.

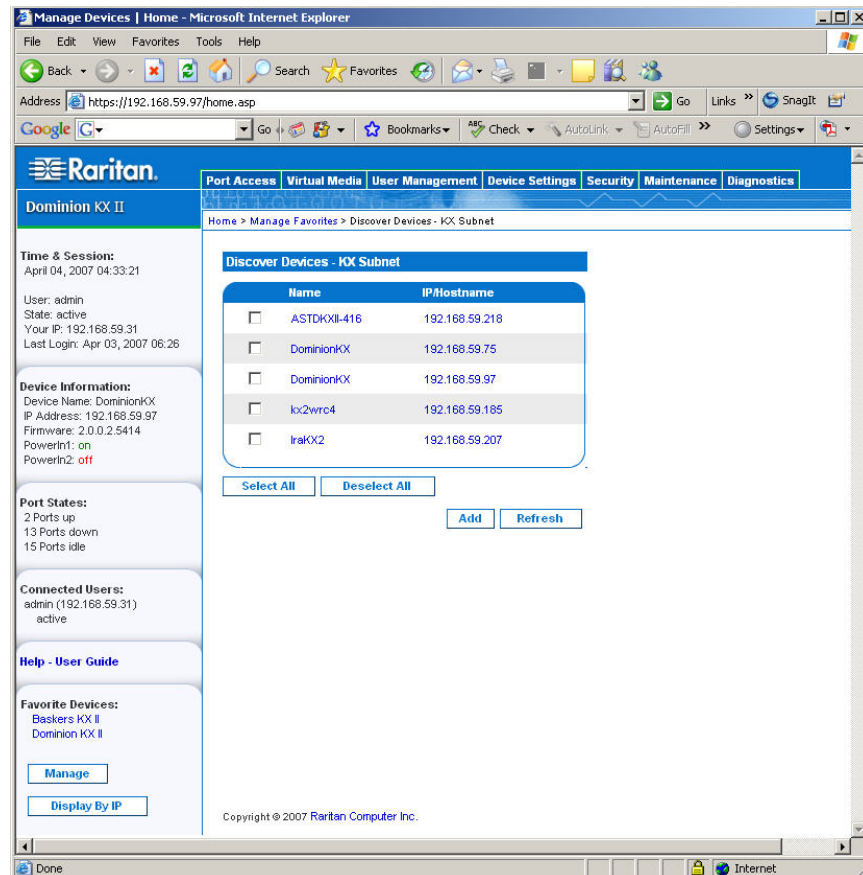


Figure 21: Discover Devices – KX Subnet

To discover devices on the KX device subnet:

1. Select **Favorites > Discover Devices – KX Subnet**. The Discover Devices – KX Subnet page opens.
2. Click **Refresh**. The list of devices on the local subnet is refreshed.

To add devices to your Favorites List:

1. Check the checkbox next to the device name/IP Address.
2. Click **Add**.

*Tip: Use the **Select All** and **Deselect All** buttons to quickly select all (or deselect all) devices in the Dominion KX II device subnet.*

To access a discovered device:

Click the device name or IP Address for that device. A new browser opens to that device.

Add New Favorite

To add a device to your favorites list:

1. Select **Manage Favorites > Add New Device to Favorites**. The Add New Favorite page opens:

The screenshot shows the 'Add New Favorite' page in a Microsoft Internet Explorer browser window. The address bar shows 'https://192.168.59.97/home.asp'. The page has a blue header with the Raritan logo and navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance, and Diagnostic. The main content area is titled 'Add New Favorite' and contains the following sections:

- Time & Session:** April 03, 2007 07:20:40; User: admin; State: 5 min idle; Your IP: 192.168.59.31; Last Login: Apr 03, 2007 04:45.
- Device Information:** Device Name: DominionKX; IP Address: 192.168.59.97; Firmware: 2.0.0.2.5414; PowerIn1: on; PowerIn2: off.
- Port States:** 16 Ports down; 16 Ports idle.
- Connected Users:** admin (192.168.59.31); 5 min idle.
- Help - User Guide**
- Favorite Devices:** Baskers KX II, Dominion KX II, Janets KXII, Prasannas KX II. Below this is a 'Manage' button.

The main form area has a blue header 'Add New Favorite' and a note 'All fields are required'. It contains three input fields: 'Description' (empty), 'IP Address' (containing '0.0.0.0'), and 'Port' (containing '5000'). At the bottom of the form are 'OK' and 'Cancel' buttons. The footer of the page says 'Copyright © 2007 Raritan Computer Inc.'.

Figure 22: Add New Favorite

2. Type a meaningful **Description**.
3. Type the **IP Address** for the device.
4. Change the discovery **Port** (if necessary).
5. Click **OK**. This device is added to your list of favorites.

Chapter 5: Accessing Target Servers

Port Access Page

After successfully logging into the Dominion KX II Remote Console, the Port Access page opens. This page lists all of the Dominion KX II ports, the connected target servers, and their status and availability. The Port Access page provides access to the target servers connected to the Dominion KX II. Target servers are servers that you want to control through the Dominion KX II unit; they are connected to the Dominion KX II ports at the back of the unit.

Note: For each connection to a target server, a *new Virtual KVM Client window is opened.*

To use the Port Access page:

1. From the KX II Remote Console, click the **Port Access** tab to open it. The Port Access page opens:

The screenshot shows the Port Access page in a web browser. The page has a sidebar with navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance, and Diagnostics. The main content area displays a table of 15 ports. A callout box labeled 'Available Targets' points to the 'Port Name' column of the table.

Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	Dominion-KX2_Port3	down	idle
4	Dominion-KX2_Port4	down	idle
5	ILTestPC	up	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	down	idle
9	Local Port	up	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
14	Dominion-KX2_Port14	down	idle
15	Dominion-KX2_Port15	down	idle

Figure 23: Port Access

The target servers are initially sorted by Port Number; you can change the display to sort on any of the columns.

- **Port Number.** Numbered from 1 to the total number of ports available for the Dominion KX II unit. Please note that ports connected to power strips will *not* be among those listed, resulting in gaps in the Port Number sequence.
 - **Port Name.** The name of the Dominion KX II port; initially set to Dominion-KX2-Port#, but you can change the name to something more descriptive. When you click on a Port Name link, the Port Action Menu is opened.
 - **Status.** The **Status** is either *up* or *down*.
 - **Availability.** The **Availability** can be *Idle*, *Connected*, *Busy*, or *Unavailable*.
2. Click the **Port Name** of the target server you want to access. The **Port Action Menu** is displayed. Refer to [Port Action Menu](#) for more information about the menu options available.
 3. Select the desired menu option from the **Port Action Menu**.

To change the display sort order:

Click the column heading you want to sort on. The list of target servers is sorted by that column.

Port Action Menu

1. When you click on a Port Name in the Port Access list, the Port Action menu is displayed. Please note that only options available for the selected port are listed in the Port Action menu:

- **Connect.** Creates a new connection to the target server. For the KX II Remote Console, a new [Virtual KVM Client](#) window is opened. For the KX II Local Console, the display switches to the target server and switches away from the local user interface. On the local port, the KX II Local Console interface must be visible in order to perform the switch.

Note: This option is not available from the KX II Remote Console for an available port if all connections are busy.

- **Switch From.** Switches from an existing connection to the selected port (target server). This menu item is available for every opened connection (up to a maximum of four for units with 4 remote users; maximum of two for units with 2 remote users; maximum of 1 for units with 1 remote user); this option is visible only when one or more Virtual KVM Clients are opened.

Note: This menu item is not available on the KX II Local Console.

- **Disconnect.** Disconnects this port and closes the Virtual KVM Client window for this target server. This menu item is available only when the port status is up and connected, or up and busy.

Note: This menu item is not available on the KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the [hotkey](#).

- **Power On.** Powers on the target server through the associated outlet. This option is visible only when there is one or more power associations to this target, when the target is off (port status is down), and when user has permission to operate this service.
- **Power Off.** Powers off the target server through the associated outlets. This option is visible only when there is one or more power associations to this target, when the target power is on (port status is up), and when user has permission to operate this service.
- **Power Cycle.** Power cycles the target server through the associated outlets. This option is visible only when there is a power association (one or more) to this target and when the user has permission to operate this service.

2. Select the desired menu option for that port to execute it.

Connecting to a Target Server

To connect to a target server:

1. From the KX II Remote Console, click the **Port Access** tab to open it. The Port Access page opens.
2. Click the **Port Name** of the target you want to access. The **Port Action Menu** is displayed:

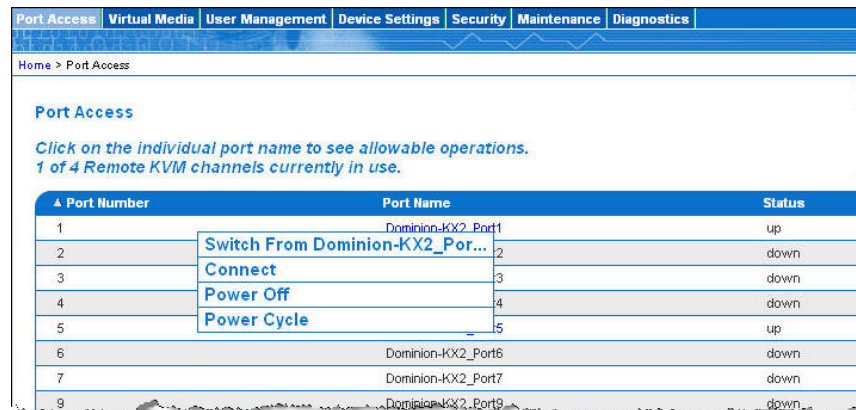


Figure 24: Port Action Menu

3. Select **Connect**. A [Virtual KVM Client](#) window opens to the target server connected to that port.

Switching between Target Servers

With the Dominion KX II, you can access several target servers. Dominion KX II provides the ability to switch from one target server to another.

Note: This feature is available in the Dominion KX II Remote Console only.

To switch between target servers:

1. While already using a target server, access the Dominion KX II Port Access page.
2. Click the **Port Name** of the target you want to access now. The **Port Action Menu** is displayed.
3. Select the **Switch From** option from the **Port Action Menu**. The [Virtual KVM Client](#) window switches to the new target server you selected.

Disconnecting Target Servers

Note: This item is not available on the KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the [hotkey](#).

To disconnect a target server:

1. Click the **Port Name** of the target you want to disconnect. The **Port Action Menu** is displayed.
2. Select the **Disconnect** option from the **Port Action Menu**. The [Virtual KVM Client](#) window closes the target window.

Tip: You can also close the Virtual KVM Client window by selecting **Connection > Exit** from the Virtual KVM menu.

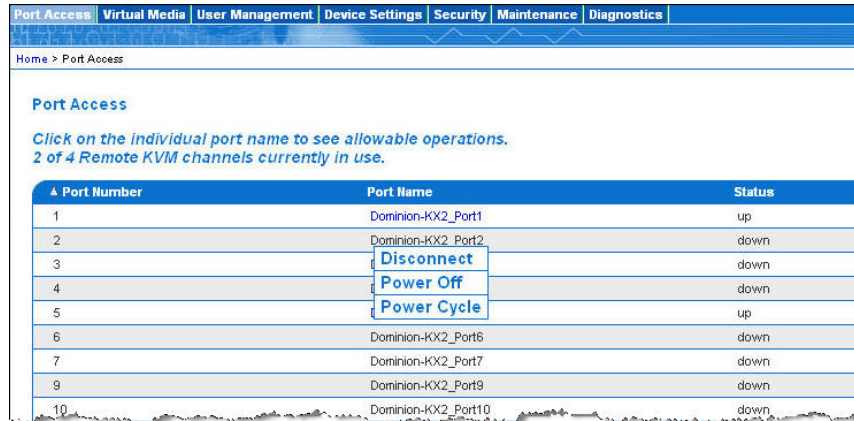
Power Controlling a Target Server

Note: These features are available only when you have made power associations. Refer to [power control](#) for more information.

Power Cycle a Target Server

To power cycle a target server:

1. From the KX II Remote Console, click the **Port Access** tab to open it. The Port Access page opens.
2. Click the **Port Name** of the appropriate target server. The **Port Action Menu** is displayed.



The screenshot shows the 'Port Access' tab selected in the top navigation bar. Below the navigation bar, there is a breadcrumb 'Home > Port Access' and a section titled 'Port Access'. A message states: 'Click on the individual port name to see allowable operations. 2 of 4 Remote KVM channels currently in use.' Below this is a table with three columns: 'Port Number', 'Port Name', and 'Status'. The table lists 10 ports. A context menu is open over 'Port 2', showing three options: 'Disconnect', 'Power Off', and 'Power Cycle'.

Port Number	Port Name	Status
1	Dominion-KX2_Port1	up
2	Dominion-KX2_Port2	down
3	Dominion-KX2_Port3	down
4	Dominion-KX2_Port4	down
5	Dominion-KX2_Port5	up
6	Dominion-KX2_Port6	down
7	Dominion-KX2_Port7	down
9	Dominion-KX2_Port9	down
10	Dominion-KX2_Port10	down

Figure 25: Port Action Menu (power options)

3. Select **Power Cycle**. A message is displayed confirming the action taken.

Power On a Target Server

To power ON a target server:

1. From the KX II Remote Console, click the **Port Access** tab to open it. The Port Access page opens.
2. Click the **Port Name** of the appropriate target server. The **Port Action Menu** is displayed.
3. Select **Power On**.

Power Off a Target Server

To power OFF a target server:

1. From the KX II Remote Console, click the **Port Access** tab to open it. The Port Access page opens.
2. Click the **Port Name** of the appropriate target server. The **Port Action Menu** is displayed.
3. Select **Power Off**.

Chapter 6: Virtual KVM Client

Whenever you access a target server using the KX II Remote Console, a Virtual KVM Client window is opened. There is one Virtual KVM Client for *each* target server connected to; these windows can be accessed via the Windows Taskbar.

Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

Note: Refreshing your HTML browser will close the Virtual KVM Client connection, so please exercise caution.

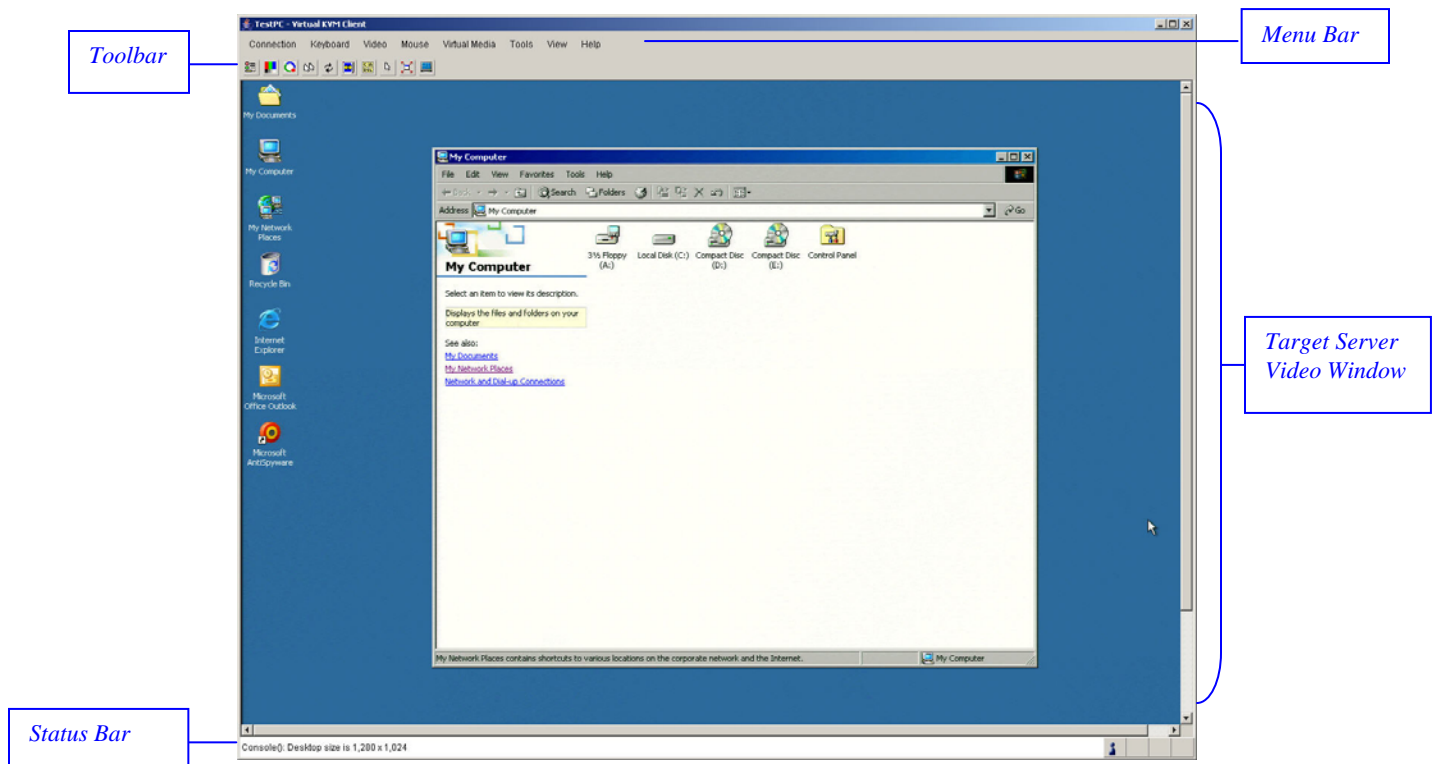


Figure 26: Virtual KVM Client Window

The features available in the Virtual KVM Client are accessible through the menu and toolbar.

FEATURE	DESCRIPTION
Menu Bar	Drop-down menus of commands and settings.
Toolbar	Shortcut buttons to frequently used features and commands.
Target Server Video Window	Target device display.
Status Bar	Real-time information on connection parameters, target server window size, concurrent connections, Caps Lock indicator, and Num Lock indicator.

Note to CC-SG Users

If you are using Dominion KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC).

Options

Menu Tree

The following diagram represents all of the menu options available in the Virtual KVM Client.

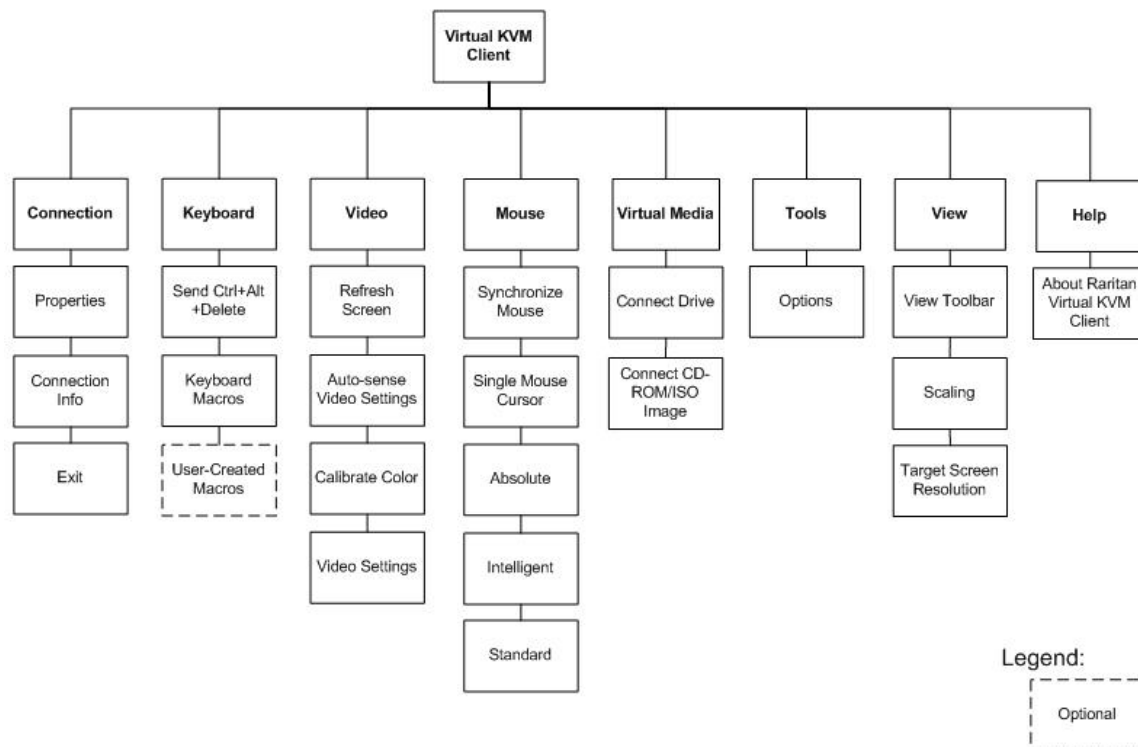


Figure 27: Virtual KVM Client Menu Tree

Toolbar

BUTTON	DESCRIPTION
	Properties
	Video settings
	Calibrate color
	Synchronize client and target server mouse cursors
	Refresh screen
	Auto-sense video
	Send Ctrl+Alt+Delete
	Toggles single/double mouse modes
	Full screen
	Resize video to fit screen

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, you will see two mouse pointers: one belonging to your remote client workstation and the other belonging to the target server. When the mouse pointer lies *within* the Virtual KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server. While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

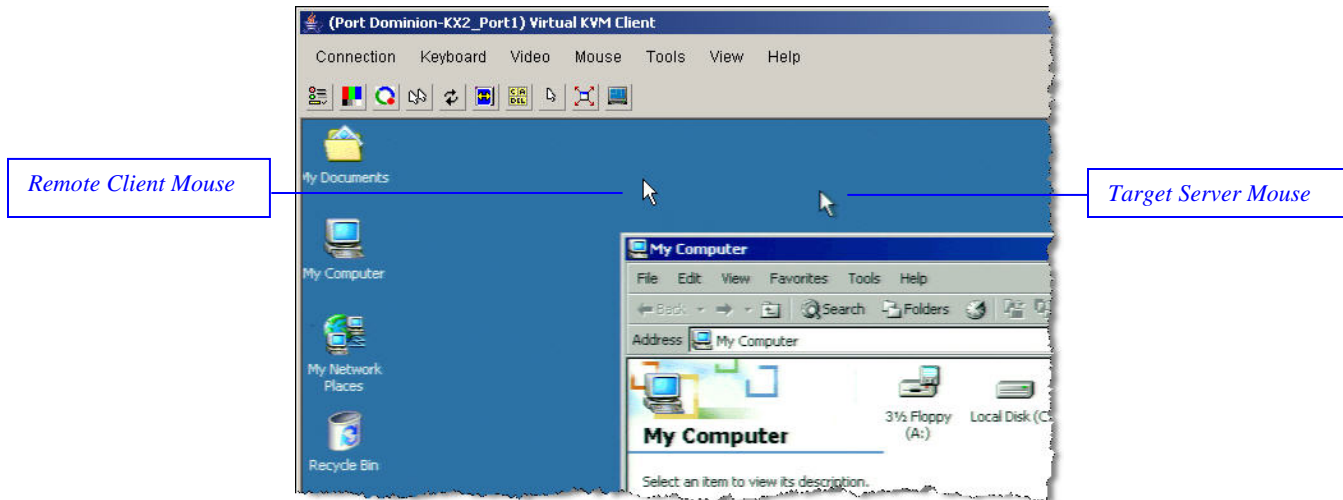




Figure 28: Dual Mouse Cursors

On fast LAN connections, you may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse). Refer to [Mouse Menu](#) for additional information about the available mouse modes.

Mouse Synchronization Tips

Be sure to follow these steps when obtaining mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the Dominion KX II. The Virtual KVM Client Connection Info dialog displays the actual values that the KX II is seeing. Please refer to [Supported Video Resolutions](#) for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Please refer to [Target Server Connection Distance and Video Resolution](#) for more information.
3. Verify that the mouse and video have been properly configured during the installation process. Please refer to [Chapter 3: Installation and Configuration](#) for complete instructions.
4. Force an auto-sense by clicking the Virtual KVM Client auto-sense  button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris target servers):
 - a. Open a terminal window.
 - b. Enter the **xset mouse 1 1** command.
 - c. Close the terminal window.
6. Click the Virtual KVM Client mouse synchronization  button.


Additional Notes for Intelligent Mouse Mode

- Be sure that there are no icons or applications in the upper left section of the screen since that is where the synchronization routine takes place.
- Do not use an animated mouse.
- Disable active desktop on target servers.

Connection Menu

Properties Dialog

The Dominion KX II dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. Dominion KX II units optimize KVM output not only for LAN use, but also for WAN and dialup use. These units can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

	Connection Properties	Manually adjust bandwidth-related options (connection speed, color depth, etc.).
---	-----------------------	--

The parameters in the Properties Dialog can be optimized to suit your needs for different operating environments.

To set the connection properties:

1. Select **Connection > Properties**. The Properties Dialog opens.

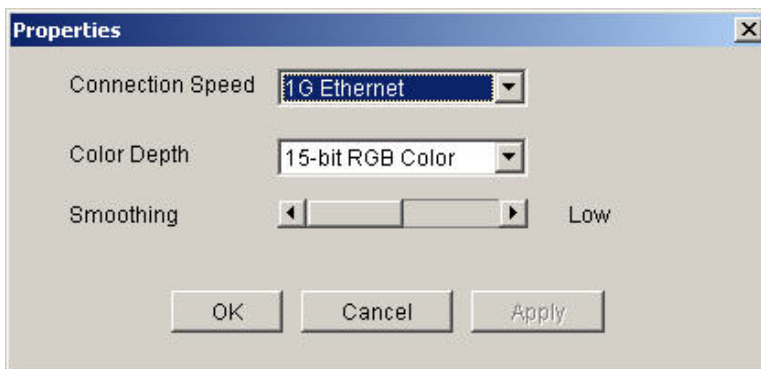


Figure 29: Properties Dialog

2. Select the **Connection Speed** from the drop-down list. Dominion KX II can automatically detect available bandwidth and not limit bandwidth use; but you can also adjust this usage according to bandwidth limitations.

Auto
1G Ethernet
100 Mb Ethernet
10 Mb Ethernet
1.5 Mb (MAX DSL/T1)
1 Mb (Fast DSL/T1)
512 Kb (Medium DSL/T1)
384 Kb (Slow DSL/T1)
256 Kb (Cable)
128 Kb (Dual ISDN)
56 Kb (ISP Modem)
33 Kb (Fast Modem)
24 Kb (Slow Modem)

Please note that these settings are an optimization for specific conditions rather than an exact speed. The client and server always attempt to deliver video as quickly as possible on the network regardless of the current network speed and encoding setting. But the system will be most responsive when the settings match the real world environment.

3. Select the **Color Depth** from the drop-down list. Dominion KX II can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.

15-bit RGB Color
8-bit RGB Color
4-bit Color
4-bit Gray
3-bit Gray
2-bit Gray
Black and White

Important: For most administrative tasks (server monitoring, reconfiguring, etc.), the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards is not necessary. Attempting to transmit such high color depths, wastes network bandwidth.

4. Use the slider to select the desired level of **Smoothing** (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.
5. Click **OK** to set these properties.

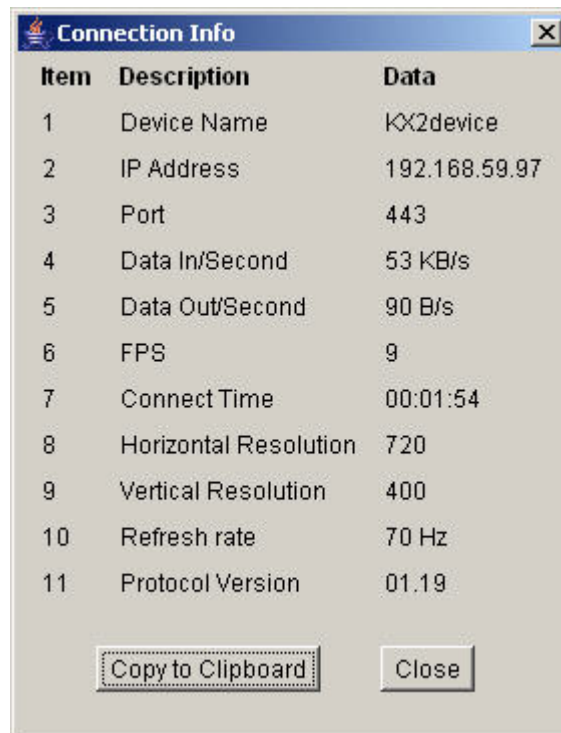
To cancel without saving changes:

Click **Cancel**.

Connection Info

To obtain information about your Virtual KVM Client connection:

Select **Connection > Connection Info**. The Connection Info window opens:



The screenshot shows a window titled "Connection Info" with a close button (X) in the top right corner. The window contains a table with three columns: "Item", "Description", and "Data". The table lists 11 items, including Device Name, IP Address, Port, Data In/Second, Data Out/Second, FPS, Connect Time, Horizontal Resolution, Vertical Resolution, Refresh rate, and Protocol Version. At the bottom of the window, there are two buttons: "Copy to Clipboard" and "Close".

Item	Description	Data
1	Device Name	KX2device
2	IP Address	192.168.59.97
3	Port	443
4	Data In/Second	53 KB/s
5	Data Out/Second	90 B/s
6	FPS	9
7	Connect Time	00:01:54
8	Horizontal Resolution	720
9	Vertical Resolution	400
10	Refresh rate	70 Hz
11	Protocol Version	01.19

Figure 30: Connection Info

The following information is displayed about the current connection:

- **Device Name.** The name of the Dominion KX II device.
- **IP Address.** The IP Address of the Dominion KX II device.
- **Port.** The KVM Communication TCP/IP Port used to access the target device.
- **Data In/Second.** Data rate in.
- **Data Out/Second.** Data rate out.
- **Connect Time.** The duration of the connect time.
- **FPS.** The frames per second transmitted for video.
- **Horizontal Resolution.** The screen resolution horizontally.
- **Vertical Resolution.** The screen resolution vertically.
- **Refresh Rate.** How often the screen is refreshed.
- **Protocol Version.** RFB Protocol version.

To copy this information:

Click **Copy to Clipboard**. The information is available to be pasted into the program of your choice.

Exit

To close the Virtual KVM Client (the target you are currently accessing):


Select **Connection > Exit**.

Keyboard Menu

Send Ctrl+Alt+Delete

Due to its frequent use, a **Ctrl+Alt+Delete** macro has been pre-programmed into the Virtual KVM Client.

This key sequence is sent to the target server to which you are currently connected. In contrast, if you were to physically press the **Ctrl+Alt+Delete** keys while using the Virtual KVM Client, the command would first be intercepted by your own PC due to the structure of the operating system, instead of sending the key sequence to the target server as intended.

	Send Ctrl+Alt+Delete	Sends a Ctrl+Alt+Delete key sequence to the target server
---	-----------------------------	--

To send a **Ctrl+Alt+Delete** key sequence to the target server:

- Select **Keyboard > Send Ctrl+Alt+Delete**, or
- Click the **Send Ctrl+Alt+Delete** button from toolbar

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server, are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the computer on which the Virtual KVM Client is running (your client PC).

Macros are stored on the client PC and are PC-specific; therefore, if you use another PC you will not see your macros. In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide. Keyboard macros created in the Virtual KVM Client are available in MPC and vice versa.

Creating a Keyboard Macro

To create a keyboard macro (add a macro):

1. Select **Keyboard > Keyboard Macros**. The Keyboard Macros window opens:

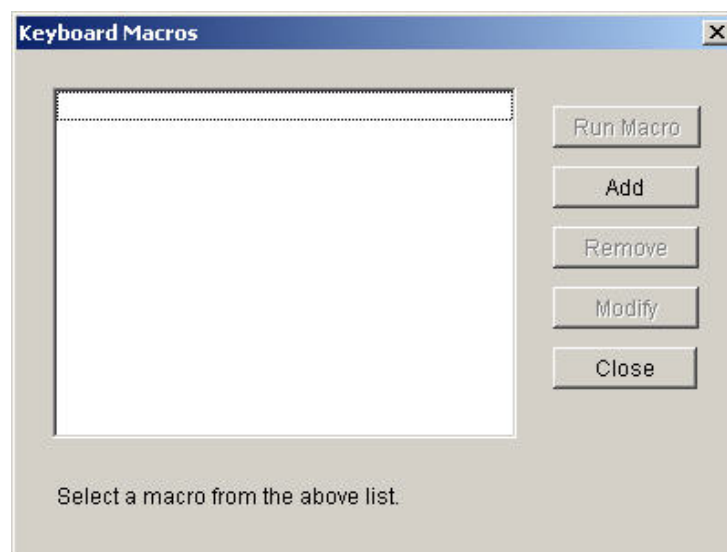


Figure 31: Keyboard Macros

2. Click **Add**. The Add Keyboard Macro window opens:

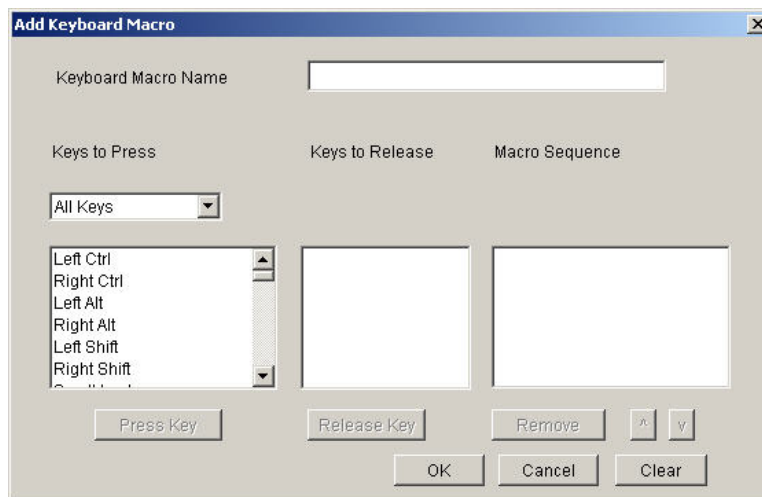


Figure 32: Add Keyboard Macro

3. Type a name in the **Keyboard Macro Name** field. This is the name that will display on the Virtual KVM Client menu bar after the macro is created. *In this example*, type **Minimize All Windows**.
4. In the **Keys to Press** drop-down list:
 - a. Scroll through and select each key for which you would like to emulate a key press (in the order in which they are to be pressed).
 - b. Click the **Press Key** button after each selection. As each key is selected, it displays in the **Keys to Release** field.

In this example, select two keys: the **Windows** key and the letter **D** key.

5. In the **Keys to Release** field:
 - a. Select each key for which you would like to emulate a key release (in the order in which they are to be released).
 - b. Click **Release Key** after each selection.

In this example, both keys pressed must also be released.

6. Review the **Macro Sequence** – which has been automatically generated using the **Keys to Press** and **Keys to Release** selections. Verify that the **Macro Sequence** is the exact key sequence you want. (To remove a step in the sequence, select it and click **Remove**.)

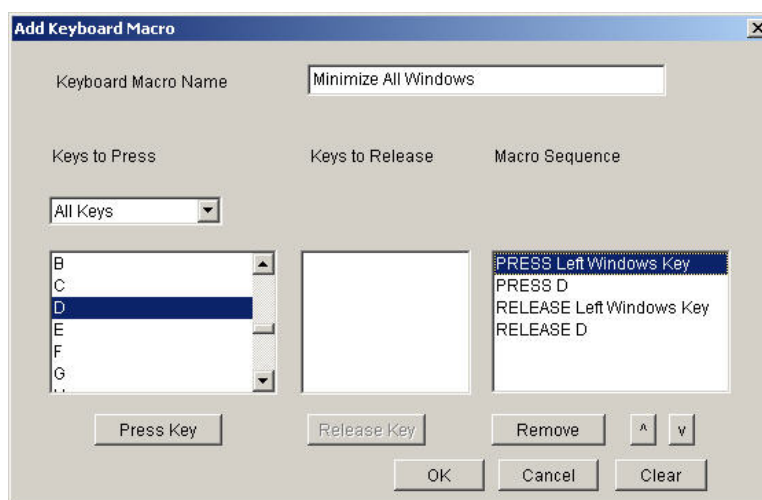


Figure 33: Keyboard Macro Example

Tip: Use the ^ and v keys to reorder the key sequence.

7. Click **OK** from the Add Keyboard Macro window to save the macro.
8. Click **Close** from the Keyboard Macros window (Figure 31). The keyboard macro created is now listed as an option from **Keyboard** menu:

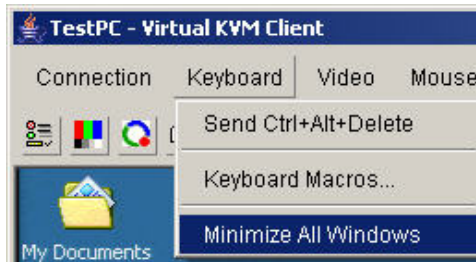


Figure 34: New Macro in Keyboard Menu

To cancel without saving changes:

Click **Cancel**.

To clear all fields and start over:

Click the **Clear** button.

Running a Keyboard Macro

Once you have created a keyboard macro, execute it by clicking on its name in the **Keyboard** menu.

To execute a macro (using this example):

Select **Keyboard > Minimize All Windows**.

An alternative method is to select the macro from the Keyboard Macros window.

To execute a macro:

1. Select **Keyboard > Keyboard Macros**. The Keyboard Macros window opens.
2. Select the macro from among those listed.
3. Click **Run Macro**.

Modifying a Keyboard Macro

To modify a macro:

1. Select **Keyboard > Keyboard Macros**. The Keyboard Macros window opens.
2. Select the macro from among those listed.
3. Click **Modify**. The Add/Edit Macro window opens.
4. Make your changes.
5. Click **OK**.

Removing a Keyboard Macro

Please exercise caution in the removal of macros; you are not prompted to confirm their deletion.

To remove a macro:

1. Select **Keyboard > Keyboard Macros**. The Keyboard Macros window opens.
2. Select the macro from among those listed.
3. Click **Remove**. The macro is deleted.

Video Menu

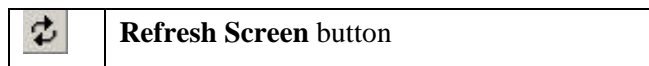
Video settings can be refreshed automatically in several ways:

- The **Refresh Screen** option forces a refresh of the video screen
- The **Auto-sense Video Settings** option automatically detects the target server's video settings
- The **Calibrate Color** option calibrates the video to enhance the colors being displayed

In addition, you can manually adjust the settings using the **Video Settings** option.

Refresh Screen

The Refresh Screen option forces a refresh of the video screen. The entire video screen is redrawn.



To refresh the video settings:

- Select **Video > Refresh Screen**, or
- Click the **Refresh Screen** button from toolbar

Auto-sense Video Settings

The Auto-sense Video Settings option forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.



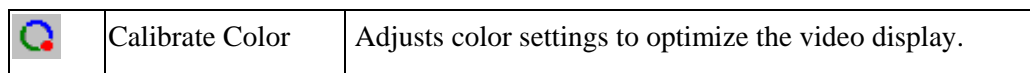
To automatically detect the video settings:

- Select **Video > Auto-sense Video Settings**, or
- Click the **Auto-Sense Video Settings** button from toolbar

A message is displayed that auto adjustment is in progress.

Calibrate Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The Dominion KX II color settings are on a target server-basis.



Note: The Calibrate Color option applies to the current connection only.

To calibrate the color:

1. Open a remote KVM connection to any target server running a graphical user interface.
2. Select **Video > Calibrate Color** (or click the Calibrate Color button). The target device screen updates its color calibration.

Video Settings

Use the Video Settings option to manually adjust the video settings.

	Video Settings	Opens Video Settings for manual adjustment of video parameters.
---	----------------	---

To change the video settings:

1. Select **Video > Video Settings**. The Video Settings window opens displaying the current settings:

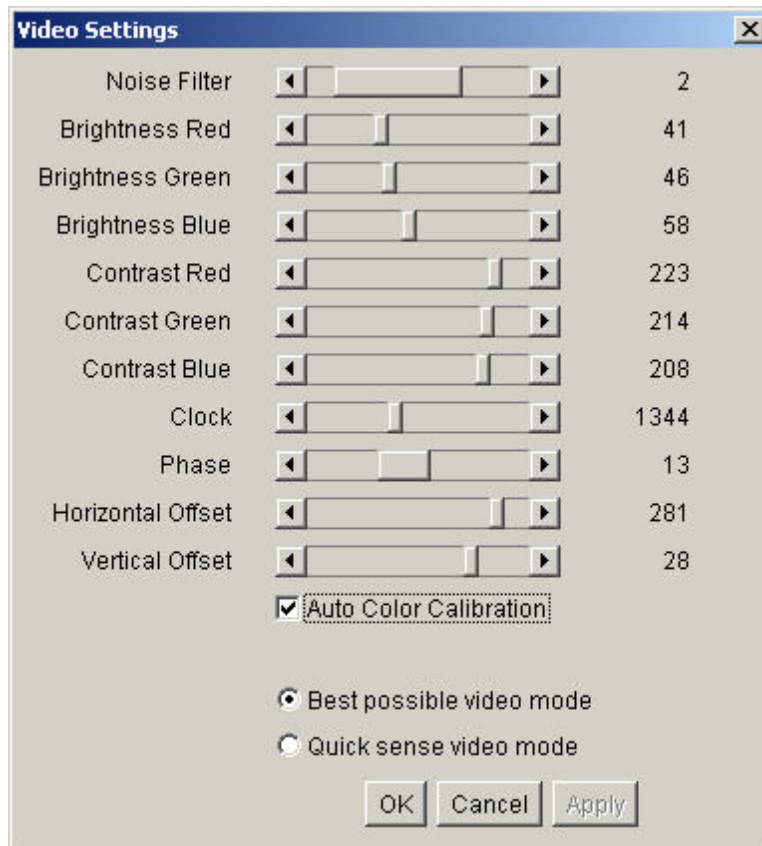


Figure 35: Video Settings

2. Use the sliders to adjust the settings to achieve the desired results (as you adjust the settings the effects are immediately visible):

- **Noise Filter.** Dominion KX II can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.

Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

- **Brightness:** Use this setting to adjust the brightness of the target server display.
 - **Red.** Controls the brightness of the red signal.
 - **Green.** Controls the brightness of the green signal.
 - **Blue.** Controls the brightness of the blue signal.

- Color Contrast Settings: Controls the contrast adjustment.
 - **Contrast Red.** Controls the red signal.
 - **Contrast Green.** Controls the green signal.
 - **Contrast Blue.** Controls the blue signal.
- If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Please exercise caution when changing the Clock and Phase settings; doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- **Clock.** Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally; odd number settings are recommended. Under most circumstances this setting should not be changed because the auto-detect is usually quite accurate.
 - **Phase.** Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.
 - Offset: Controls the on-screen positioning:
 - **Horizontal Offset.** Controls the horizontal positioning of the target server display on your monitor.
 - **Vertical Offset.** Controls the vertical positioning of the target server display on your monitor.
 - **Auto Color Calibration.** Check this option if you would like automatic color calibration.
 - **Video Sensing:** Select the video sensing mode:
 - **Best possible video mode:** Dominion KX II will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
 - **Quick sense video mode:** With this option, the Dominion KX II will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
3. Click **Apply**. The Video Settings are changed.

***Note:** Some Sun background screens, such as screens with very dark borders, may not center precisely on certain Sun servers. Use a different background or place a lighter colored icon in the upper left corner of the screen.*

To cancel with saving your changes:

Click **Cancel**.

Mouse Menu

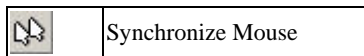
When controlling a target server, the KX II Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server. You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode and properly configured, these two mouse cursors will align. If you experience difficulty with mouse synchronization, refer to [Configure Target Servers](#).

When there are two mouse cursors, the Dominion KX II offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

Synchronize Mouse

In dual mouse mode, the Synchronize Mouse option forces realignment of the target server mouse pointer with Virtual KVM Client mouse pointer.

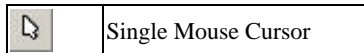


To synchronize the mouse:

- Select **Mouse > Synchronize Mouse**, or
- Click the Synchronize Mouse button from the toolbar

Single Mouse Cursor

Single Mouse Cursor enters single mouse mode, in which only the target server mouse cursor is shown; the local PC mouse pointer no longer appears on-screen. While in single mouse mode, the Synchronize Mouse option is not available (there is no need to synchronize a single mouse cursor).



To enter single mouse mode:

- Select **Mouse > Single Mouse Cursor**, or
- Click the Single/Double Mouse Cursor button from the toolbar

To exit single mouse mode:

1. When entering single mouse mode, the following message is displayed. Click **OK**.

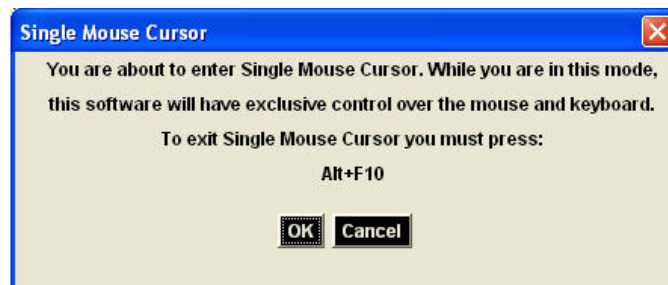


Figure 36: Single Mouse Cursor Message

2. Press **Alt+F10** from your keyboard to exit single mouse mode.

Standard

This is the standard mouse synchronization algorithm using relative mouse positions. Standard mouse mode requires that acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized. Standard mouse mode is the default.

To enter standard mouse mode:

Select **Mouse > Standard**

Intelligent

In Intelligent mouse mode, the Dominion KX II can detect the target mouse settings and synchronize the mouse pointers accordingly, allowing mouse acceleration on the target. In this mode, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

For additional information on Intelligent Mouse mode, refer to the *Raritan Multi-Platform Client User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization)* available on Raritan’s Website <http://www.raritan.com/support/productdocumentation>, or on the *Raritan User Manuals & Quick Setup Guides CD ROM* included with your Dominion KX II shipment.

To enter intelligent mouse mode:

Select **Mouse > Intelligent**

Absolute

***Note:** Absolute Mouse Synchronization is available for use with the Virtual Media-enabled USB CIM (D2CIM-VUSB) only.*

In this mode, absolute coordinates are used to keep the client and target pointers in sync, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports; the mouse moves to the exact location on the target server.

To enter absolute mouse mode:

Select **Mouse > Absolute**

Virtual Media

Refer to the chapter on [Virtual Media](#) for complete information about setting up and using virtual media.

Tools Menu

Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client: synchronize mouse when in dual mouse mode, enable logging, keyboard type, and the exit target screen resolution mode hotkey.

To set the tools options:

1. Select **Tools > Options**. The Options window opens:

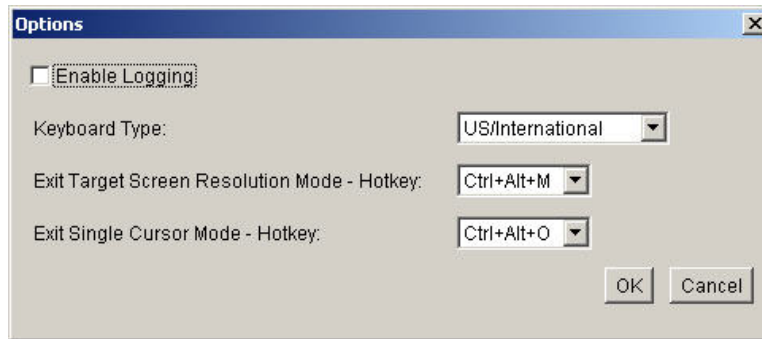


Figure 37: (Tools) Options

2. Check the **Enable Logging** checkbox *only* if directed to by Technical Support. This option creates a log file in your home directory.
3. Select the **Keyboard Type** from the drop-down list (if necessary). The options include:
 - US/International
 - French (France)
 - German (Germany)
 - Japanese
 - United Kingdom
 - Korean (Korea)
4. **Exit Target Screen Resolution Mode - Hotkey**. When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hotkey used for exiting this mode; select from the drop-down list.
5. **Exit Single Cursor Mode - Hotkey**. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hotkey used to exit single cursor mode and bring back the client mouse cursor; select from the drop-down list.
6. Click **OK**.

View Menu

View Toolbar

You can use the Virtual KVM client with or without the toolbar display.

To toggle the display of the toolbar (on and off):

Select **View > View Toolbar**.

Scaling

Scaling your target window allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

To toggle scaling (on and off):

Select **View > Scaling**.

Target Screen Resolution

When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. The hotkey used for exiting this mode is specified in the Options dialog (default is **Ctrl+Alt+M**).

To enter target screen resolution:

Select **View > Target Screen Resolution**.

To exit target screen resolution mode:

Press the hotkey configured in Figure 37. The default is **Ctrl+Alt+M**.

***Note to CC-SG Users:** Target Screen Resolution is disabled; full screen mode is available only when the Dominion KX II device is not under CC-SG management.*

Help Menu

About Raritan Virtual KVM Client

This menu option provides version information about the Virtual KVM Client should you require assistance from Raritan technical support.

To obtain version information:

Select **Help > About Raritan Virtual KVM Client**.

Chapter 7: Virtual Media

Overview

Virtual media extends KVM capabilities by enabling target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is essentially *mounted virtually* by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

Virtual media provides the ability to perform additional tasks remotely, such as:

- transferring files
- running diagnostics
- installing or patching applications
- complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.

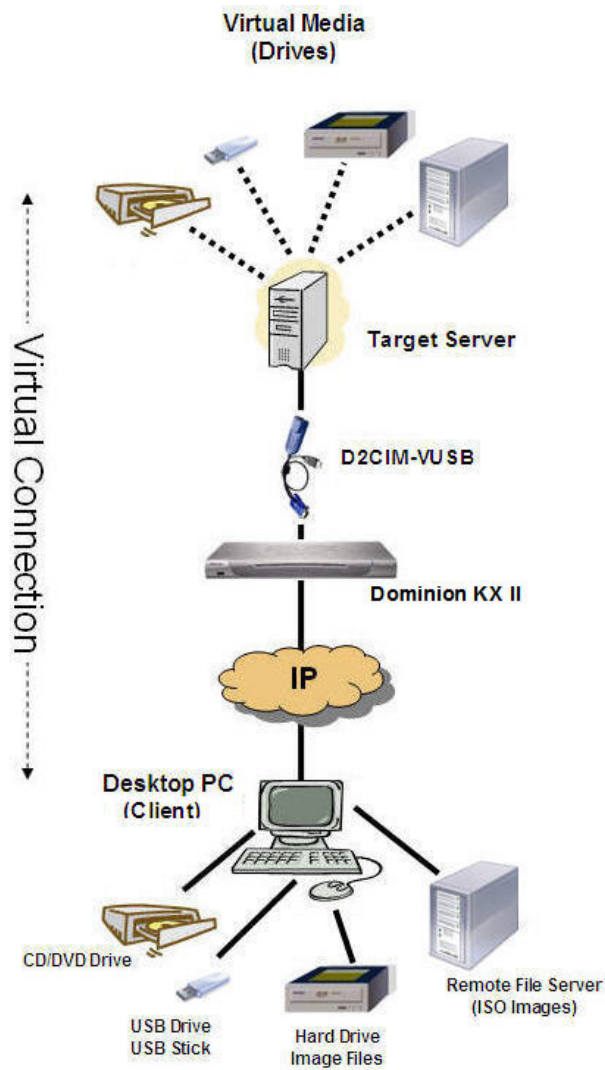


Figure 38: Virtual Media Connection

Prerequisites for Using Virtual Media

The following conditions must be met in order to use virtual media:

Dominion KX II

- For users requiring access to virtual media, KX permissions must be set to allow access to the relevant ports, as well as virtual media access (**VM Access** port permission) for those ports. Port permissions are set at the group-level; please refer to [Setting Port Permissions](#) for more information.
- (Optional) If you want to use PC-Share, [VM Share Mode](#) must also be enabled in the Security Settings page.

Client PC

- Certain virtual media options require administrative privileges on the client PC (e.g., drive redirection of complete drives).

***Note:** If you are using Microsoft Vista, turn User Account Control **off**: Control Panel > User Accounts > User Account Control > turn off.*

*If you would prefer not to change Vista account permissions, run Internet Explorer as an administrator. To do this, click on the Start Menu, locate IE, right click it and select **Run as Administrator**.*

- USB 2.0 ports are both faster and preferred.

Target Server

- Target servers must support USB connected drives.
- Target servers running Windows 2000 must have all of the recent patches installed.

Using Virtual Media

With the Dominion KX II virtual media feature, you can mount up to two drives (of different types). These drives are accessible for the *duration* of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed.

To use virtual media:

1. Connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done *prior to* attempting to access this media.
2. Verify that the appropriate [prerequisites](#) are met.
3. (**File server ISO images only**) If you plan to access file server ISO images, identify those file servers and images through the Dominion KX II Remote Console [File Server Setup page](#).
4. [Open a KVM session](#) with the appropriate target server.
5. Connect to the virtual media.

FOR:	SELECT THIS VM OPTION:
Local drives	Connect Drive
Local CD/DVD drives	Connect CD-ROM/ISO Image
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

6. Upon completion of your tasks, [disconnect the virtual media](#).

Opening a KVM Session

To open a KVM session:

1. Open the Port Access page from the Dominion KX II Remote Console.

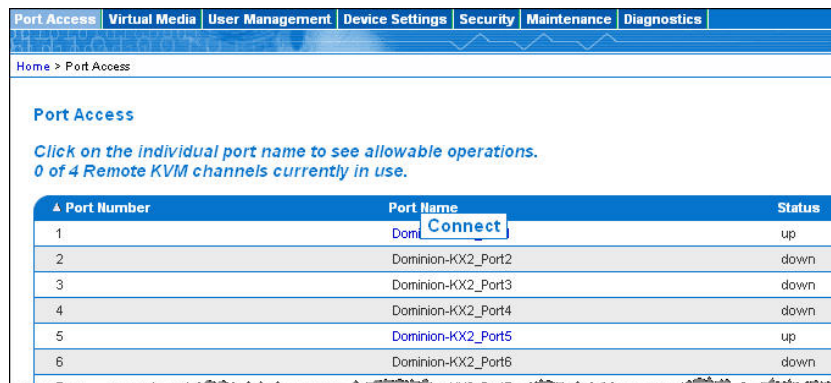


Figure 39: Open KVM Session

2. Connect to the target server from the Port Access page:
 - a. Click the **Port Name** for the appropriate server.
 - b. Select the **Connect** option from the Port Action Menu.

The target server opens in a [Virtual KVM Client](#) window.

Connecting to Virtual Media

Local Drives

This option mounts an *entire* drive; the entire disk drive is *mounted virtually* onto the target server. Use this option for hard drives and external drives only; it does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which **Read-Write** is available.

***Note:** Target servers running certain version of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (e.g., the local C drive) has been redirected to them. If this occurs, close the KX II Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.*

To access a drive on the client computer:

1. From the Virtual KVM Client, select **Virtual Media > Connect Drive**. The Map Virtual Media Drive dialog opens:

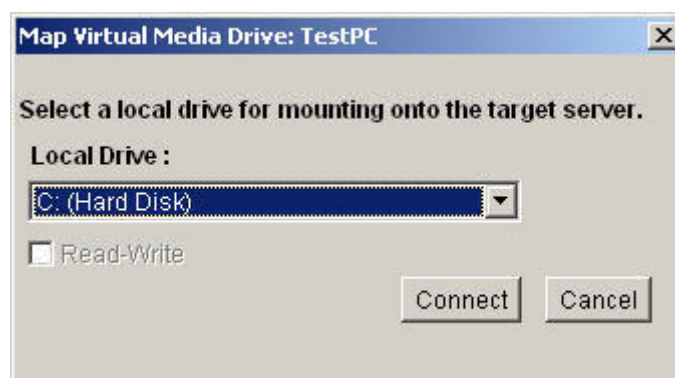


Figure 40: Map Virtual Media Drive

2. Select the drive from the **Local Drive** drop-down list.
3. If you want read and write capabilities, check the **Read-Write** option checkbox. This option is disabled for non-removable drives. Please refer to the [conditions when read-write is not available](#) for more information. When checked, you will be able to read or write the connected USB disk.

WARNING: Enabling Read-Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require write access, leave this option unchecked.

4. Click **Connect**. The media will be mounted on the target server virtually. You can access the media just like any other drive

Conditions when Read-Write is not Available

Virtual media read-write is not available in the following situations:

- For all hard drives.
- When the drive is write-protected.
- When the user does not have read-write permission:
 - Port Permission **Access** is set to *None* or *View*
 - Port Permission **VM Access** is set to *Read-Only* or *Deny*

CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

To access a CD-ROM, DVD-ROM, or ISO image:

1. From the Virtual KVM Client, select **Virtual Media > Connect CD-ROM/ISO Image**. The Map Virtual Media CD/ISO Image dialog opens:

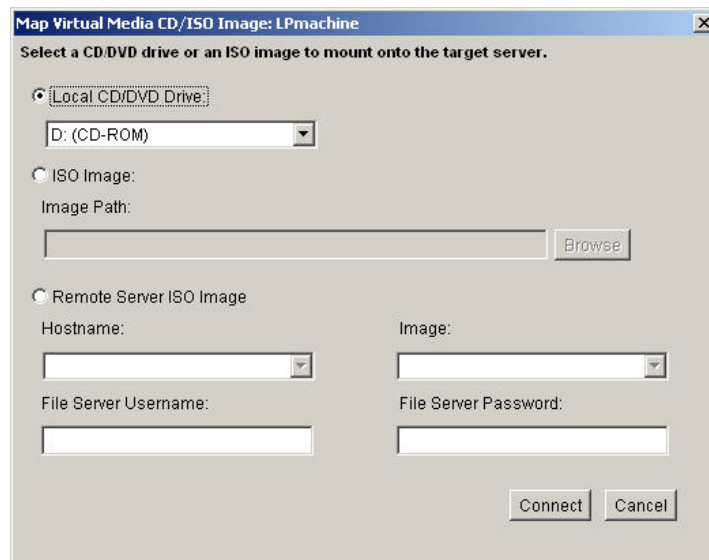


Figure 41: Map Virtual Media CD/ISO Image

2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Select the **Local CD/DVD Drive** option.
 - b. Select the drive from the **Local CD/DVD Drive** drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
 - c. Click **Connect**.

3. For ISO images:
 - a. Select the **ISO Image** option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click the **Browse** button.
 - c. Navigate to the path containing the disk image you want to use and click **Open**. The path is populated in the **Image Path** field.
 - d. Click **Connect**.
4. For remote ISO images on a file server:
 - a. Select the **Remote Server ISO Image** option.
 - b. Select **Hostname** and **Image** from the drop-down lists. The file servers and image paths available are those that you configured using the [File Server Setup](#) page. Only items you configured using the Dominion KX II File Server Setup page will be in the drop-down list.
 - c. **File Server Username**. Username required for access to the file server.
 - d. **File Server Password**. Password required for access to the file server (field is masked as you type).
 - e. Click **Connect**.

The media will be mounted on the target server virtually. You can access the media just like any other drive.

Disconnecting Virtual Media

To disconnect the Virtual Media drives:

- For local drives, select **Virtual Media > Disconnect Drive**
- For CD-ROM, DVD-ROM, and ISO images, select **Virtual Media > Disconnect CD-ROM/ISO Image**

***Note:** In addition to disconnecting the virtual media using the **Disconnect** option, simply closing the KVM connection closes the Virtual Media as well.*

File Server Setup (File Server ISO Images Only)

Note: This feature is only required when using virtual media to access file server ISO images.

Use the Dominion KX II Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using Dominion KX II Virtual Media. File server ISO image(s) specified here will become available for selection in the **Remote Server ISO Image Hostname** and **Image** drop-down lists (in the [Map Virtual Media CD/ISO Image dialog](#)).

To designate file server ISO images for virtual media access:

1. Select **Virtual Media** from the Dominion KX II Remote Console. The File Server Setup page opens:

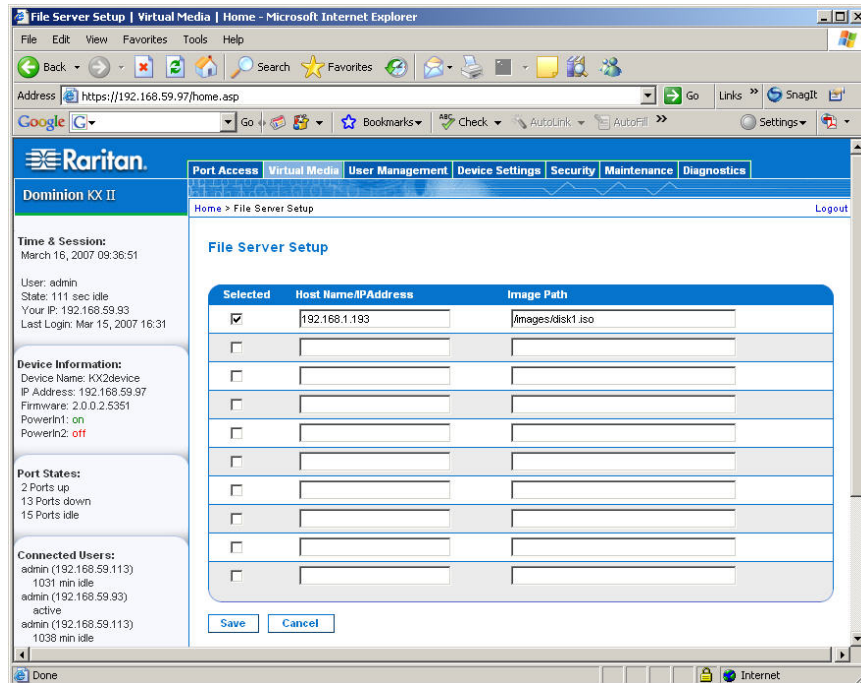


Figure 42: File Server Setup

2. Input information about the file server ISO images that you want to access:
 - **Host Name/IP Address.** Host name or IP Address of the file server.
 - **Image Path.** Full path name of the location of the ISO image.
3. Check the **Selected** checkbox for all media that you want accessible as virtual media.
4. Click **Save**. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.

To cancel without saving:

Click **Cancel**.

Chapter 8: User Management

The User Management menu is organized as follows: User List, Add New User, User Group List, Add New User Group, Change Password, and Authentication Settings.

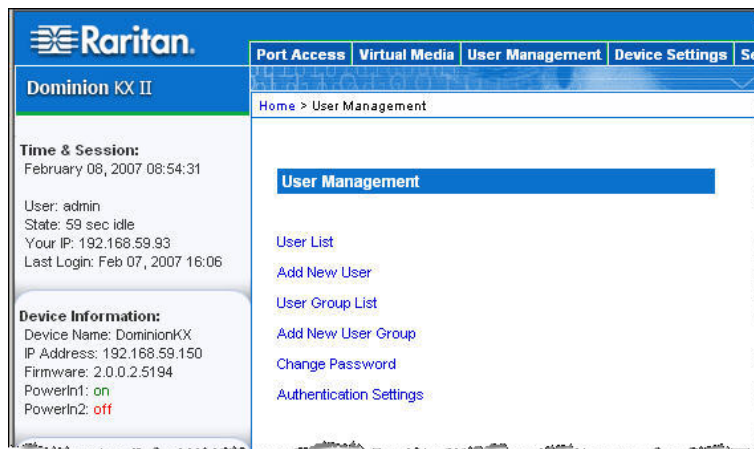


Figure 43: User Management Menu

USE:	TO:
User List	Display an alphabetical list of all users; add, modify, or delete users.
Add New User	Add new users; modify user information.
User Group List	Display an alphabetical list of all user groups; add, modify, or delete user groups.
Add New User Group	Add new user groups; modify user group information.
Change Password	Change password for a specific user.
Authentication Settings	Configure the type of authentication used for access to the Dominion KX II.

User List

The User List page displays a list of all users including their Username, Full Name, and User Group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can also add, modify, or delete users.

To view the list of users:

Select **User Management > User List**. The User List page opens:

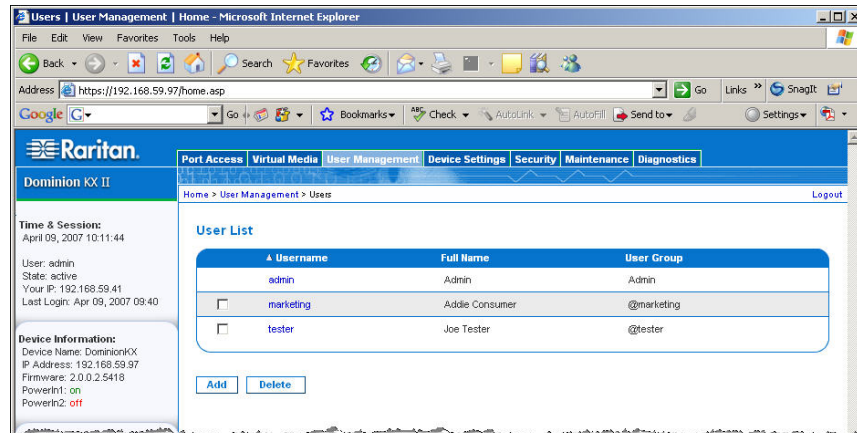


Figure 44: User List

To add a new user:

Click the **Add** button. The User page opens. For complete information about the User page, refer to [Add New User](#).

To modify an existing user:

1. Locate the user from among those listed.
2. Click on the **Username**. The User page opens. For complete information editing the user, refer to [Modify Existing User](#).

To delete a user:

1. Select the user from among those listed by checking the checkbox to the left of the Username.
2. Click **Delete**.
3. You are prompted to confirm the deletion. Click **OK**.

Add New User

It is a good idea to define user groups *before* creating Dominion KX II users, because when you add a user, you must assign that user to an *existing* user group. From the User page, you can add new users, modify user information, and reactivate users that have been deactivated.

Note: A username can be deactivated (**Active** checkbox is cleared) when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings screen. Refer to [Security Settings](#) for more information.

To add a new user:

1. Open the User page using one of these methods:
 - Select **User Management > Add New User**, or
 - Click the **Add** button from the User List page

The screenshot shows a web browser window displaying the Raritan User Management interface. The browser's address bar shows 'https://192.168.59.97/home.asp'. The page has a blue header with the Raritan logo and navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, and Maintenance. The 'User Management' tab is selected, and the breadcrumb trail is 'Home > User Management > User'. The main content area is titled 'User' and contains a form with the following fields: Username (text input), Full Name (text input), Password (text input), Confirm Password (text input), User Group (dropdown menu), and an Active checkbox (checked). There are 'OK' and 'Cancel' buttons at the bottom of the form. On the left side of the page, there is a sidebar with sections: Time & Session (March 02, 2007 18:02:19), User: admin, State: active, Your IP: 192.168.59.93, Last Login: Mar 02, 2007 17:04; Device Information (Device Name: DominionKX, IP Address: 192.168.59.97, Firmware: 2.0.0.2.5282, PowerIn1: on, PowerIn2: off); Port States (2 Ports up, 13 Ports down, 15 Ports idle); and Connected Users.

Figure 45: User Page

2. Type a unique name in the **Username** field (up to 16 characters).
3. Type the person's full name in the **Full Name** field (up to 64 characters).
4. Type a password in the **Password** field; retype the password in the **Confirm Password** field (up to 64 characters).
5. Select the group from the **User Group** drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group). If you do not want to associate this user with an existing User Group, select **Individual Group** from the drop-down list.

For more information about permissions for an Individual Group, refer to [Set Permissions for Individual Group](#).

6. To activate this user, check the **Active** checkbox. The default is activated (enabled).
7. Click **OK**.

Modify Existing User

To modify an existing user:

1. From the User page (Figure 45), change the appropriate fields. (Refer to [Add New User](#) for information about how to get access the User page.)
2. Click **OK**.

User Group List

User groups are used with local and remote authentication (via RADIUS or LDAP). It is a good idea to define user groups *before* creating individual users, because when you add a user, you must assign that user to an *existing* user group.

The User Group List page displays a list of all user groups, which can be sorted in ascending or descending order by clicking on the Group Name column heading. From the User Group List page, you can also add, modify, or delete user groups.

To list the user groups:

Select **User Management > User Group List**. The User Group List page opens:

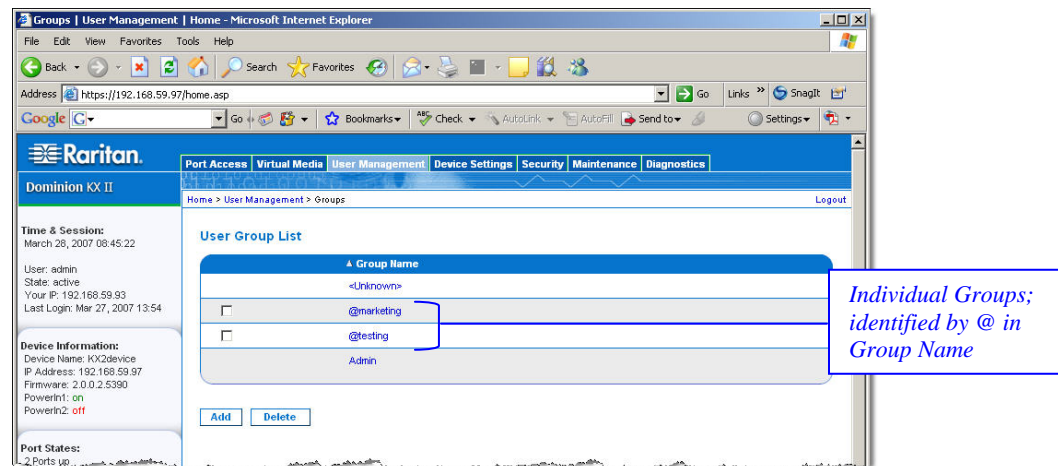


Figure 46: User Group List

To add a new user group:

Click the **Add** button. The Group page opens. For complete information about the Group page, refer to [Add New User Group](#).

To modify an existing user group:

1. Locate the user group from among those listed.
2. Click on the Group Name. The Group page opens. For complete information editing the group, refer to [Modify Existing User Group](#).

To delete a user group:

Important: Before deleting a group, ensure that no users are assigned to it, or those users will also be deleted.

Tip: To determine the users belonging to a particular group, sort the User List (Figure 44) by User Group.

1. Select a group from among those listed by checking the checkbox to the left of the Group Name.
2. Click **Delete**.
3. You are prompted to confirm the deletion. Click **OK**.

Add New User Group

To add a new user group:

1. Open the Group page using one of these methods:
 - Select **User Management > Add New User Group**, or
 - Click the **Add** button from the User Group List page

Raritan. Dominion KX II

Port Access Virtual Media **User Management** Device Settings Security Maintenance Diagnostics

Home > User Management > Group Logout

Time & Session:
March 26, 2007 09:23:08
User: admin
State: 1 min idle
Your IP: 192.168.59.93
Last Login: Mar 23, 2007 15:37

Device Information:
Device Name: KX2device
IP Address: 192.168.59.97
Firmware: 2.0.0.2.5390
PowerIn1: on
PowerIn2: off

Port States:
16 Ports down
16 Ports idle

Connected Users:
admin (192.168.59.93)
1 min idle

[Help - User Guide](#)

Favorite Devices:
Baskers KX II
Dominion KX II
Janets KX II
Prasannas KX II

[Manage](#)

[Display By IP](#)

Group

Group Name *

Permissions

☐ Device Settings
☐ Diagnostics
☐ Maintenance
☐ PC-Share
☐ Security
☐ User Management

Port Permissions

Port	Access	VM Access	Power Control
Dominion-KX2_Port1	None	Deny	Deny
Dominion-KX2_Port2	None	Deny	Deny
Dominion-KX2_Port3	None	Deny	Deny
Dominion-KX2_Port4	None	Deny	Deny
Dominion-KX2_Port5	None	Deny	Deny
Dominion-KX2_Port6	None	Deny	Deny
Dominion-KX2_Port7	None	Deny	Deny
Dominion-KX2_Port8	None	Deny	Deny
Dominion-KX2_Port9	None	Deny	Deny
Dominion-KX2_Port10	None	Deny	Deny
Dominion-KX2_Port11	None	Deny	Deny
Dominion-KX2_Port12	None	Deny	Deny
Dominion-KX2_Port13	None	Deny	Deny
Dominion-KX2_Port14	None	Deny	Deny
Dominion-KX2_Port15	None	Deny	Deny
Dominion-KX2_Port16	None	Deny	Deny

☐ Set All to None
☐ Set All to View
☐ Set All to Control

☐ Set All VM Access to Deny
☐ Set All VM Access to Read-Only
☐ Set All VM Access to Read-Write

☐ Set All Power to Deny
☐ Set All Power to Access

IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

[Append](#) [Insert](#) [Replace](#) [Delete](#)

[OK](#) [Cancel](#)

Copyright © 2007 Raritan Computer Inc.

Figure 47: Group Page

The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

2. Type a descriptive name for the new user group into the **Group Name** field.
3. Set the **Permissions** for the group. Check the boxes before the permissions you want to assign to *all of the users belonging* to this group. Refer to [Setting Permissions](#) for more information.
4. Set the **Port Permissions**. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to [Setting Port Permissions](#) for more information.

5. [Set the IP ACL](#) (optional). This feature limits access to the Dominion KX II device by specifying IP addresses; it applies **only** to users belonging to a specific group, unlike the [IP Access Control](#) list feature which applies to **all** access attempts to the device (and takes priority).
6. Click **OK**.

***Note:** Several administrative functions are available within MPC and from the Dominion KX II Local Console; these functions are available only to members of the default ADMIN group.*

Setting Permissions

Important: Checking the “User Management” checkbox allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.

PERMISSION	DESCRIPTION
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setup
Diagnostics	Network interface status, network statistics, ping host, trace route to host, KX diagnostics
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL
User Management	User and group management, remote authentication (LDAP/RADIUS), login settings

Setting Port Permissions

For each server port, you can specify the type of access, the type of access to the virtual media, and the power control. Please note that the default setting for all permissions is disabled.

ACCESS		VM ACCESS		POWER CONTROL	
Option	Description	Option	Description	Option	Description
None*	Denied access completely	Deny*	Virtual media permission is denied altogether for the port	Deny*	Denied access completely
View	View the video (but not interact with) the connected target server	Read-Only	Virtual media access is limited to read access only	Access	Complete access
Control	Control the connected target server	Read-Write	Complete access (read, write) to virtual media		

* Default setting

Tip: Use the checkboxes to quickly set all the permissions the same for every port.

Group-based IP ACL (Access Control List)

Important: Please exercise caution when using group-based IP access control. It is possible to be locked out of your Dominion KX II if your IP Address is within a range that has been denied access.

This feature limits access to the Dominion KX II device by users in the selected group to specific IP addresses. This feature applies **only** to users belonging to a specific group, unlike the IP Access Control List feature which applies to **all** access attempts to the device, is processed first, and takes priority. Refer to [IP Access Control](#) for more information.

Important: IP Address 127.0.0.1 is used by the Dominion KX II Local Port. When creating an Access Control List, if 127.0.0.1 is within the range of IP Addresses that are blocked, then you will not have access to the Dominion KX II local port.

Use the IP ACL section of the Group page to add, insert, replace, and delete IP access control rules on a group-level basis.

Figure 48: Group-based IP Access Control List

To add (append) rules:

1. Type the starting IP Address in the **Starting IP** field.
2. Type the ending IP Address in the **Ending IP** field.
3. Select the **Action** from the available options:
 - **Accept.** IP Addresses specifying accept are allowed access to the Dominion KX II device.
 - **Drop.** IP Addresses specifying drop are denied access to the Dominion KX II device.
4. Click **Append**. The rule is added to the bottom of the rules list.
5. Repeat steps 1 through 4 for each rule you want to enter.

To insert a rule:

1. Type a **Rule #**. A Rule # is required when using the Insert command.
2. Populate the **Starting IP** and **Ending IP** fields.
3. Select the **Action** from the drop-down list.
4. Click **Insert**. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

To replace a rule:

1. Specify the **Rule #** you want to replace.
2. Populate the **Starting IP** and **Ending IP** fields.
3. Select the **Action** from the drop-down list.
4. Click **Replace**. Your new rule replaces the original rule with the same Rule #.

To delete a rule:

1. Specify the **Rule #** you want to delete.
2. Click **Delete**.
3. You are prompted to confirm the deletion. Click **OK**.

Important: ACL rules are evaluated in the order in which they are listed. For instance, in the example shown here, if the two ACL rules were reversed, Dominion would accept no communication at all.

The screenshot shows a web interface for configuring IP ACLs. At the top is a blue header bar labeled "IP ACL". Below it is a table with four columns: "Rule #", "Starting IP", "Ending IP", and "Action".

Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP

Below the table, there are four input fields for a new rule, followed by a dropdown menu currently set to "ACCEPT". At the bottom of the interface are four buttons: "Append", "Insert", "Replace", and "Delete".

Figure 49: IP ACL Example

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

Modify Existing User Group

Note: All permissions are enabled (and cannot be changed) for the Admin group.

To modify an existing user group:

1. From the Group page, change the appropriate fields and set the appropriate permissions.

Raritan. Dominion KX II

Port Access | Virtual Media | **User Management** | Device Settings | Security | Maintenance | Diagnostics

Home > User Management > Group Logout

Group

Group Name: @marketing

Permissions

☐ Device Settings
☐ Diagnostics
☐ Maintenance
☐ PC-Share
☐ Security
☐ User Management

Port Permissions

Port	Access	VM Access	Power Control
Dominion-KX2_Port1	None	Deny	Deny
Dominion-KX2_Port2	None	Deny	Deny
Dominion-KX2_Port3	None	Deny	Deny
Dominion-KX2_Port4	None	Deny	Deny
Dominion-KX2_Port5	None	Deny	Deny
Dominion-KX2_Port6	None	Deny	Deny
Dominion-KX2_Port7	None	Deny	Deny
Dominion-KX2_Port8	None	Deny	Deny
Dominion-KX2_Port9	None	Deny	Deny
Dominion-KX2_Port10	None	Deny	Deny
Dominion-KX2_Port11	None	Deny	Deny
Dominion-KX2_Port12	None	Deny	Deny
Dominion-KX2_Port13	None	Deny	Deny
Dominion-KX2_Port14	None	Deny	Deny
Dominion-KX2_Port15	None	Deny	Deny
Dominion-KX2_Port16	None	Deny	Deny

☐ Set All to None
 ☐ Set All VM Access to Deny
 ☐ Set All Power to Deny
☐ Set All to View
 ☐ Set All VM Access to Read-Only
 ☐ Set All Power to Access
☐ Set All to Control
 ☐ Set All VM Access to Read-Write

IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Copyright © 2007 Raritan Computer Inc.

Figure 50: Modify Group

2. Set the **Permissions** for the group. Check the boxes before the permissions you want to assign to *all of the users belonging* to this group. Refer to [Setting Permissions](#) for more information.
3. Set the **Port Permissions**. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to [Setting Port Permissions](#) for more information.
4. Set the **IP ACL** (optional). This feature limits access to the Dominion KX II device by specifying IP addresses. Refer to [Group-based IP Access Control List](#) for more information.
5. Click **OK**.

Set Permissions for Individual Group

To set permissions for an individual user group:

1. Locate the user from among the groups listed. Individual groups can be identified by the @ in the **Group Name**.
2. Click on the **Group Name**. The Group page (Figure 50) opens.
3. Select the appropriate permissions.
4. Click **OK**.

Change Password

To change your password:

1. Select **User Management > Change Password**. The Change Password page opens:

Figure 51: Change Password

2. Type your current password in the **Old Password** field.
3. Type a new password in the **New Password** field; retype the new password in the **Confirm New Password** field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and [special characters](#).
4. Click **OK**.
5. You will receive confirmation that the password was successfully changed. Click **OK**.

Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, refer to [Security Settings – Strong Passwords](#).

Authentication Settings

From the Authentication Settings page you can configure the type of authentication used for access to your Dominion KX II. Refer to [Authentication vs. Authorization](#) for more information about how authentication and authorization operate and differ.

***Note:** Even if you select remote authentication (LDAP or RADIUS), local authentication is still used.*

To configure authentication:

1. Select **User Management > Authentication Settings**. The Authentication Settings page opens:

Raritan

Port Access | Virtual Media | **User Management** | Device Settings | Security | Maintenance | Diagnostics

Home > User Management > Authentication Settings Logout

Authentication Settings

☒ Local Authentication
☐ LDAP

Primary LDAP Server
 Secondary LDAP Server

Secret Phrase
 Confirm Secret Phrase

☐ Enable Secure LDAP

Port
 Secure LDAP Port

Certificate File Browse...

DN of Administrative User
 User Search DN

Type of External LDAP Server
 Generic LDAP server

Active Directory Domain

☐ RADIUS

Primary RADIUS Server
 Shared Secret

Authentication Port
 Accounting Port

Timeout (in seconds)
 Retries

Secondary RADIUS Server
 Shared Secret

Authentication Port
 Accounting Port

Timeout (in seconds)
 Retries

Global Authentication Type
 PAP

OK Reset To Defaults Cancel

Copyright © 2007 Raritan Computer Inc.

Figure 52: Authentication Settings

2. Select the option for the authentication protocol you want to use (**Local Authentication**, **LDAP**, or **RADIUS**). Selecting the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you selected **Local Authentication**, proceed to step 6.
4. If you selected **LDAP**, read the section entitled [Implementing LDAP Remote Authentication](#) for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you selected **RADIUS**, read the section entitled [Implementing RADIUS Remote Authentication](#) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. When finished, click **OK** to save.

To cancel without saving changes:

Click **Cancel**.

To return to factory defaults:

Click the **Reset to Defaults** button.

Implementing LDAP Remote Authentication

Lightweight Directory Access Protocol (LDAP) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft Active Directory functions natively as an LDAP authentication server.

To use the LDAP authentication protocol, input the following information:



The form is titled "LDAP" with a gear icon. It contains the following fields and controls:

- Primary LDAP Server**: A text input field.
- Secondary LDAP Server**: A text input field.
- Secret Phrase**: A text input field.
- Confirm Secret Phrase**: A text input field.
- Enable Secure LDAP**: A checkbox.
- Port**: A text input field with the value "389".
- Secure LDAP Port**: A text input field with the value "636".
- Certificate File**: A text input field followed by a "Browse..." button.
- DN of Administrative User**: A text input field.
- User Search DN**: A text input field.
- Type of External LDAP Server**: A dropdown menu with "Generic LDAP server" selected.
- Active Directory Domain**: A text input field.

Figure 53: Authentication Settings (LDAP)

1. Type the IP Address or DNS name of your LDAP remote authentication server in the **Primary LDAP Server** field. When the **Enable Secure LDAP** option is checked, the DNS name must be used.
2. (Optional) Type the IP Address or DNS name of your backup LDAP server in the **Secondary LDAP Server** field. When the **Enable Secure LDAP** option is checked, the DNS name must be used. Please note that the remaining fields share the same settings with the **Primary LDAP Server** field.
3. Type the server secret (password) required to authenticate against your remote authentication server in the **Secret Phrase** field and again in the **Confirm Secret Phrase** field.
4. Check the **Enable Secure LDAP** checkbox if you would like to use SSL; the **Secure LDAP Port** field is enabled. Secure Sockets Layer (SSL) is a cryptographic protocol which allows Dominion KX II to communicate securely with the LDAP server.
5. The default **Port** is 389. Either use the standard LDAP TCP port or specify another port.
6. The default **Secure LDAP Port** is 636. Either use the default port or specify another port. This field is enabled when the **Enable Secure LDAP** box is checked.
7. **Certificate File**. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP server. Use the **Browse** button to navigate to the certificate file. This field is enabled when the **Enable Secure LDAP** option is checked.

8. **DN of administrative User.** Distinguished Name of administrative user; consult your authentication server administrator for the appropriate values to type into this field. An example DN of administrative User value might be:
“cn=Administrator,cn=Users,dc=testradius,dc=com”.
9. **User Search DN.** This describes the name you want to bind against the LDAP, and where in the database to begin searching for the specified Base DN. An example Base Search value might be: “cn=Users,dc=raritan,dc=com”. Consult your authentication server administrator for the appropriate values to enter into these fields.
10. **Type of external LDAP server.** Select from among the options available:
 - **Generic LDAP Server.**
 - **Microsoft Active Directory.** Active Directory is an implementation of LDAP directory services by Microsoft for use in Windows environments.
11. **Active Directory Domain.** Type the name of the Active Directory Domain.

Returning User Group Information from Active Directory Server

The Dominion KX II supports user authentication to Active Directory (AD) *without* requiring that users be defined locally on the KX II. This allows Active Directory user accounts and passwords to be maintained *exclusively* on the AD server. Authorization and AD user privileges are controlled and administered through the standard KX II policies and user group privileges (that are applied locally to AD user groups).

***Note:** If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, Dominion KX II still supports this configuration, and you do not need to perform the following operations. Please refer to [Appendix B: Updating the LDAP Schema](#) for information about updating the AD LDAP schema.*

To enable your AD server on the Dominion KX II:

1. Using Dominion KX II, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as: KVM_Admin, KVM_Operator.
2. On your Active Directory server, create new groups with the *same* group names as in the previous step.
3. On your AD server, assign the Dominion KX II users to the groups created in step 2.
4. From the Dominion KX II, enable and configure your AD server properly. Please refer to [Implementing LDAP Remote Authentication](#).

Important Notes:

- Group Name is case sensitive.
- The Dominion KX II provides the following default groups which can not be changed or deleted: Admin and <Unknown>. Please verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match a KX II group configuration, the Dominion KX II automatically assigns the group of <Unknown> to users who authenticate successfully.

Implementing RADIUS Remote Authentication

Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

To use the RADIUS authentication protocol:

RADIUS

Primary Radius Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Secondary Radius Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Global Authentication Type
PAP

Figure 54: Authentication Settings (RADIUS)

1. Type the IP Address of your primary and (optional) secondary remote authentication servers in the **Primary Radius Server** and **Secondary Radius Server** fields, respectively.
2. Type the server secret used for authentication (in the **Shared Secret** fields). The shared secret is a character string that must be known by both the Dominion KX II and the RADIUS server to allow them to communicate securely. It is essentially a password.
3. **Authentication Port.** The default authentication port is 1812; change as required.
4. **Accounting Port.** The default accounting port is 1813; change as required.
5. **Timeout (in seconds).** The default timeout is 1 second; change as required. The timeout is the length of time the Dominion KX II waits for a response from the RADIUS server before sending another authentication request.
6. **Retries.** The default number of retries is 3; change as required. This is the number of times the Dominion KX II will send an authentication request to the RADIUS server.
7. **Global Authentication Type.** Select from among the options in the drop-down list:
 - **PAP.** With PAP, passwords are sent as plain text. PAP is not interactive; the username and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
 - **CHAP.** With CHAP authentication can be requested by the server at any time. CHAP provides more security than PAP.

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the Dominion KX II device determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS *FILTER-ID*. The *FILTER-ID* should be formatted as follows:

```
Raritan:G{GROUP_NAME}
```

where *GROUP_NAME* is a string, denoting the name of the group to which the user belongs.

RADIUS Communication Exchange Specifications

The Dominion KX II unit sends the following RADIUS attributes to your RADIUS server:

ATTRIBUTE	DATA
LOGIN	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2):	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) – Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
LOGOUT	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

Chapter 9: Device Management

The Device Settings menu is organized as follows: Network, Date/Time, Event Management (Settings and Destinations), Power Supply Setup, Port Configuration, and Local Port Settings (Dominion KX II Local Console only).

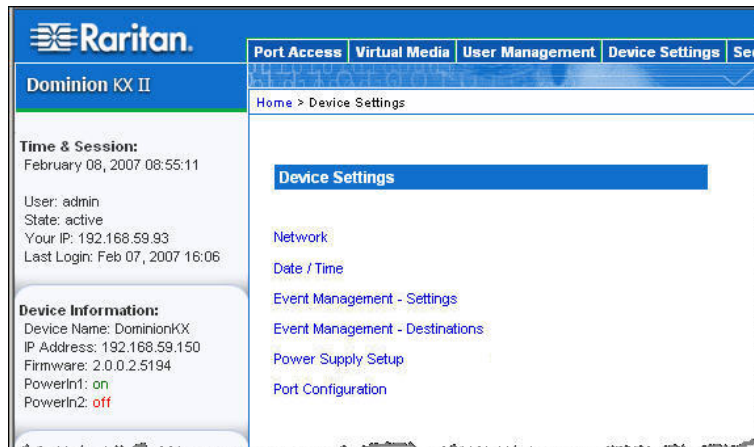


Figure 55: Device Settings Menu

USE:	TO:
Network	Customize the network configuration for the Dominion KX II.
Date/Time	Set date, time, time zone, and Network Time Protocol (NTP).
Event Management - Settings	Configure SNMP and Syslog.
Event Management - Destinations	Select which system events to track and where to send this information.
Power Supply Setup	Configure auto-detection of the Dominion KX II power supplies.
Port Configuration	Configure KVM ports, power CIMs, and outlets.
Local Port Settings	Configure local port; <i>Dominion KX II Local Console only</i> .

Network Settings

Use the Network Settings page to customize the network configuration (e.g., IP Address, discovery port, and LAN interface parameters) for your Dominion KX II unit.

Important: Dominion KX II must be rebooted for new network settings to take effect. Before changing the network configuration, ensure that there are no other active user connections to the device; all connections will be dropped when the KX II unit reboots.

Basically, there are two ways to setup your IP Configuration:

- **None.** This option is the recommended option (**Static IP**). Since the Dominion KX II is part of your network infrastructure, you most likely do not want its IP Address to change frequently. This option allows you to set the network parameters.
- **DHCP.** The IP Address is automatically assigned by a DHCP server.

To change the network configuration:

1. Select **Device Settings > Network**. The Network Settings page opens.

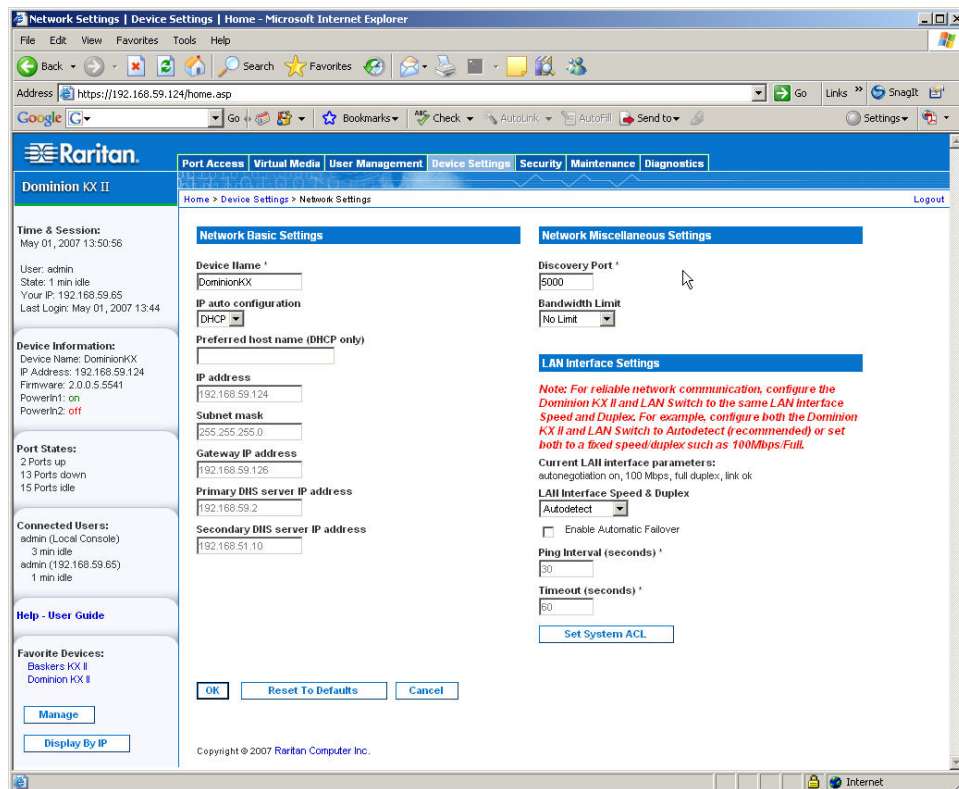


Figure 56: Network Settings

2. Update the Network Basic Settings. Refer to [Network Basic Settings](#) for more information about each of the fields.
3. Update the Network Miscellaneous Settings. Refer to [Network Miscellaneous Settings](#) for more information about each of the fields.
4. Update the LAN Interface Settings. Refer to [LAN Interface Settings](#) for more information about each of the fields.
5. Click **OK** to set these configurations. If your changes require rebooting the device, a reboot message appears.

To cancel without saving changes:

Click **Cancel**.

To reset to factory defaults:

Click **Reset to Defaults**.

Network Basic Settings

Figure 57: Network Settings (Network Basic Settings)

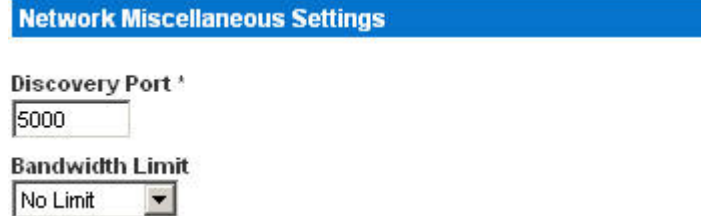
- **Device Name.** Type a unique name for the device (up to 16 characters; spaces are not allowed). Name your device so you can easily identify it. The default name for a Dominion KX II unit is: “**DominionKX**”. Remote users will also see this name. However, if an MPC user has created a Connection Profile for this device, that user will see the **Description** field from the Profile instead.
- **IP auto configuration.** Select from among the options available in the drop-down list:
 - **None.** Use this option if you do not want an auto IP configuration and prefer to set the IP Address yourself (static IP). This is the default and recommended option.

*If this option is selected for the **IP auto configuration**, the following Network Basic Settings fields are enabled, allowing you to manually set the IP configuration.*

- ♦ **IP Address.** The default IP Address is 192.168.0.192.
- ♦ **Subnet Mask.** The default subnet mask is 255.255.255.0.
- ♦ **Gateway IP Address.** The IP Address for the gateway (if one is used).
- ♦ **Primary DNS Server IP Address.** The primary Domain Name Server used to translate names into IP Addresses.
- ♦ **Secondary DNS Server IP Address.** The secondary Domain Name Server used to translate names into IP Addresses (if one is used).
- **DHCP.** Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

- ♦ If DHCP is used, enter the **Preferred host name (DHCP only)**. Up to 63 characters.

Network Miscellaneous Settings



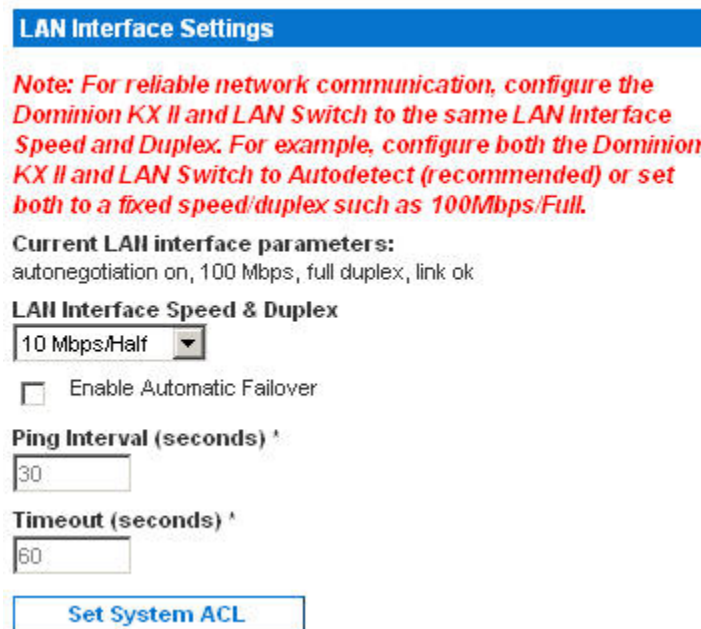
The screenshot shows the 'Network Miscellaneous Settings' window. It contains two fields: 'Discovery Port' with a text input box containing '5000', and 'Bandwidth Limit' with a dropdown menu currently set to 'No Limit'.

Figure 58: Network Settings (Network Miscellaneous Settings)

- **Discovery Port.** Dominion KX II discovery occurs over a single, configurable TCP Port. The default is **Port 5000**, but you can configure it to use any TCP port *except* 80 and 443. To access the KX II unit from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or a non-default port configured here. For more information, refer to [Configure Network Firewall Settings](#).
- **Bandwidth Limit.** The default is *no limit*. Select from among the options in the drop-down list to set a maximum amount of bandwidth that can be consumed by this Dominion KX II unit (for all sessions). The options include: No Limit, 100 Megabit, 10 Megabit, 5 Megabit, 2 Megabit, 512 Kilobit, 256 Kilobit, and 128 Kilobit.

***Note:** Lower bandwidth may result in slower performance.*

LAN Interface Settings



The screenshot shows the 'LAN Interface Settings' window. At the top, a red note states: 'Note: For reliable network communication, configure the Dominion KX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.' Below this, the 'Current LAN interface parameters:' section shows 'autonegotiation on, 100 Mbps, full duplex, link ok'. The 'LAN Interface Speed & Duplex' dropdown is set to '10 Mbps/Half'. There is an unchecked checkbox for 'Enable Automatic Failover'. The 'Ping Interval (seconds)' is set to '30' and the 'Timeout (seconds)' is set to '60'. At the bottom is a button labeled 'Set System ACL'.

Figure 59: Network Settings (LAN Interface Settings)

- The current parameter settings are identified in the **Current LAN interface parameters** field.

- **LAN Interface Speed & Duplex.** Select from among the speed and duplex combinations available.

Autodetect	<i>Default option</i>
10 Mbps/Half	
10 Mbps/Full	
100 Mbps/Half	
100 Mbps/Full	
1000 Mbps/Full	<i>Gigabit</i>

- **Half-duplex** provides for communication in both directions, but only one direction at a time (not simultaneously).
- **Full-duplex** allows communication in both directions simultaneously.

Note: Occasionally there are problems running at 10 Mbps in either half or full duplex. If you are experiencing problems, please try another speed and duplex.

Please refer to [Network Speed Settings](#) for more information.

- **Enable Automatic Failover.** Check this checkbox to allow Dominion KX II to automatically recover its network connection using a second network port if the active network port fails. When this option is enabled, the following two fields are used:
 - **Ping Interval (seconds).** Ping interval determines how often Dominion KX II checks the status of the network connection (setting this too low may cause excess network traffic). The default Ping Interval is 30 seconds.
 - **Timeout (seconds).** Timeout determines how long a network port must be “dead” before the switch is made. Both network ports must be connected to the network and this option must be checked for Automatic Failover to function. The default Timeout is 60 seconds.

Note: The default Ping Interval and Timeout generate a condition that when the KX device tries to switch over, remote sessions will be dropped and must be re-established. Reducing these intervals to much lower values will allow remote sessions to stay connected, but will result in increased network traffic.

- **Set System ACL.** Click this button to set a global-level Access Control List for your Dominion KX II by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The [IP Access Control](#) page opens.

Note: These ACL values are global, affecting the Dominion KX II unit as a whole. You can also create ACLs on a group-level basis. For example, you can create an “Outsourced Vendors” user group that is permitted to access Dominion KX II only from a given IP address range (refer to [Group-based IP ACL](#) for more information on how to create group-specific Access Control Lists).

Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the Dominion KX II. There are two ways to do this:

- Manually set the date and time, or
- Synchronize with a Network Time Protocol (NTP) Server.

To set the date and time:

1. Select **Device Settings > Date/Time**. The Date/Time Settings page opens:

Figure 60: Date/Time Settings

2. Select *your time zone* from the **Time Zone** drop-down list.
3. Select the method you would like to use to set the date and time:
 - **User Specified Time**. Select this option to input the date and time manually.
 - **Synchronize with NTP Server**. Select this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
4. For the **User Specified Time** option, enter the date and time as follows:
 - a. Select the **Month** from the drop-down list.
 - b. Type the **Day** of the Month.
 - c. Type the **Year** in yyyy format.
 - d. Enter the **Time** in hh:mm format (using a 24-hour clock).
5. For the **Synchronize with NTP Server** option:
 - a. Enter the IP address of the **Primary Time server**.
 - b. (Optional) Enter the IP address of the **Secondary Time server**.
6. Click **OK**.

Event Management

The Dominion KX II Event Management feature provides a set of screens for enabling and disabling the distribution of system events to SNMP Managers, Syslog, and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

Event Management – Settings

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. Dominion KX II offers SNMP Agent support through Event Management. Refer to [SNMP Agent Configuration](#) and [SNMP Trap Configuration](#) for more information about SNMP Agents and Traps.

To configure SNMP (enable SNMP logging):

1. Select **Device Settings > Event Management - Settings**. The Event Management - Settings page opens:

The screenshot shows the 'Event Management - Settings' page for a Dominion KX II device. The browser window title is 'Event Management - Settings | Device Settings | Home - Microsoft Internet Explorer'. The address bar shows 'https://192.168.59.97/home.asp'. The page has a navigation bar with tabs: Port Access, Virtual Media, User Management, Device Settings (selected), Security, Maintenance, and Diagnostics. The breadcrumb trail is 'Home > Device Settings > Event Management - Settings'.

Left Sidebar:

- Time & Session:** April 09, 2007 10:30:17; User: admin; State: 46 sec idle; Your IP: 192.168.59.41; Last Login: Apr 09, 2007 09:53
- Device Information:** Device Name: DominionKX; IP Address: 192.168.59.97; Firmware: 2.0.0.2.5418; PowerIn1: on; PowerIn2: off
- Port States:** 2 Ports up; 13 Ports down; 15 Ports idle
- Connected Users:** admin (192.168.59.41) 46 sec idle
- Help - User Guide**
- Favorite Devices:** Baskers KX II, Dominion KX II; Buttons: Manage, Display By IP

Main Content Area:

SNMP Configuration

☐ SNMP Logging Enabled

Name:

Contact:

Location:

Agent Community String:

Type:

Destination IP	Port #	Community
<input type="text" value="162"/>	<input type="text" value="162"/>	<input type="text" value="public"/>
<input type="text" value="162"/>	<input type="text" value="162"/>	<input type="text" value="public"/>
<input type="text" value="162"/>	<input type="text" value="162"/>	<input type="text" value="public"/>
<input type="text" value="162"/>	<input type="text" value="162"/>	<input type="text" value="public"/>
<input type="text" value="162"/>	<input type="text" value="162"/>	<input type="text" value="public"/>

[Click here to view the Dominion KX II SNMP MIB](#)

SysLog Configuration

☐ Enable Syslog Forwarding

IP Address:

Buttons: OK, Reset To Defaults, Cancel

Figure 61: Event Management – Settings

2. Check the **Enable SNMP Logging** option; this enables the remaining SNMP fields.

3. In the **Name**, **Contact**, and **Location** fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the KX II Console interface, a contact name related to this unit, and where the Dominion unit is physically located, respectively.
4. Type the **Agent Community String** (the Dominion unit's string). An SNMP community is the group that devices and management stations running SNMP belong to; it helps define where information is sent. The community name is used to identify the group; an SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read-Write using the **Type** drop-down list.
6. Configure up to five SNMP managers by specifying their **Destination IP**, **Port #**, and **Community**.
7. Click on the **Click here to view the Dominion-KX2 SNMP MIB** link to access the SNMP Management Information Base.
8. Click **OK**.

Syslog Configuration

The image shows a 'SysLog Configuration' dialog box. It has a blue title bar with the text 'SysLog Configuration'. Below the title bar, there is a checkbox labeled 'Enable Syslog Forwarding'. Underneath the checkbox, the text 'IP Address' is displayed above a text input field.

Figure 62: Syslog Configuration

To configure the Syslog (enable Syslog forwarding):

1. Check the **Enable Syslog Forwarding** option to log the device's messages to a remote Syslog server.
2. Type the IP Address of your Syslog server in the **IP Address** field.
3. Click **OK**.

To cancel without saving changes:

Click **Cancel**.

To reset to factory defaults:

Click the **Reset To Defaults** button.

Event Management – Destinations

System events, if enabled, can generate SNMP notification events (traps), or can be logged to Syslog or Audit Log. Use the Event Management - Destinations page to select which system events to track and where to send this information.

Note: *SNMP traps will only be generated if the SNMP Logging Enabled option is checked; Syslog events will only be generated if the Enable Syslog Forwarding option is checked. Both of these options are in the [Event Management – Settings](#) page.*

To select events and their destinations:

1. Select **Device Settings > Event Management - Destinations**. The Event Management - Destinations page opens:

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit Log
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	Begin CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Activity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Access Login	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Access Logout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	Connection Lost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Session Timeout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	VM Image Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	VM Image Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	CM Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	CM Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	CM Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	CM Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Group Administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Added	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Group Administration	User Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Deleted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Group Added	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Group Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Group Deleted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Reset To Defaults Cancel

Copyright © 2007 Raritan Computer Inc.

Figure 63: Event Management - Destinations

System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.

2. Check the checkboxes for those **Event** line items you want to enable or disable, and where you want to send the information.

Tip: Enable or disable entire Categories by checking or clearing the Category line checkboxes, respectively.

3. Click **OK**.

To cancel without saving changes:

Click **Cancel**.

To reset to factory defaults:

Click the **Reset To Defaults** button.

SNMP Agent Configuration

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP managers. Use the Event Logging page to configure the SNMP connection between the Dominion KX II (SNMP Agent) and an SNMP manager.

SNMP Trap Configuration

SNMP provides the ability to send traps, or notifications, to advise an administrator when one or more conditions have been met. The following table lists the Dominion KX II SNMP traps:

TRAP NAME	DESCRIPTION
cimConnected	A CIM is plugged into to the Dominion KX II port.
cimDisconnected	A CIM is either unplugged from the Dominion KX II port or powered-off.
cimUpdateCompleted	CIM firmware update process completed.
cimUpdateStarted	CIM firmware update process started.
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The Dominion KX II has completed update via an RFP file.
deviceUpgradeStarted	The Dominion KX II has begun update via an RFP file.
ethernetFailover	An Ethernet failover was detected and restored on a new Ethernet interface.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.
groupAdded	A group has been added to the KX II system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The KX has completed its reboot.
rebootStarted	The KX has begun to reboot, either through cycling power to the system or by a warm reboot from the OS.
securityViolation	Security violation.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the KX II and has been authenticated.
userLogout	A user has successfully logged out of the KX II properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of <i>any</i> user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Power Supply Setup Page

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Use the Power Supply Setup page to specify whether you are using one or both of the power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail. For example, if power supply number one fails, the power LED at the front of the unit will turn red.

To enable automatic detection for the power supplies in use:

1. Select **Device Settings > Power Supply Setup**. The Power Supply Setup page opens:

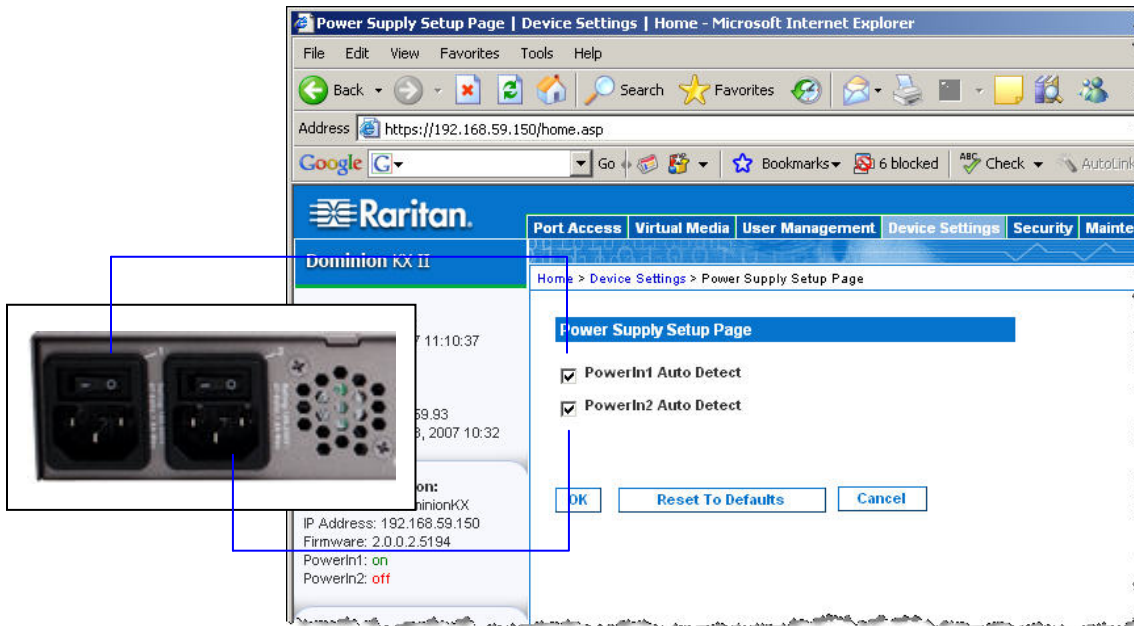


Figure 64: Power Supply Setup

2. If you are plugging power input into power supply number one (left-most power supply at the back of the unit), then check the **PowerIn1 Auto Detect** option.
3. If you are plugging power input into power supply number two (right-most power supply at the back of the unit), then check the **PowerIn2 Auto Detect** option.
4. Click **OK**.

Note: If either of these checkboxes is checked and power input is not actually connected, the power LED at the front of the unit displays red.

To turn off the automatic detection:

Clear the checkbox for the appropriate power supply.

To reset to factory defaults:

Click the **Reset To Defaults** button.

To cancel without saving changes:

Click the **Cancel** button.

Note: Dominion KX II does NOT report power supply status to CommandCenter. Dominion I (generation 1), however, does report power supply status to CommandCenter.

Port Configuration Page

The Port Configuration page displays a list of the Dominion KX II ports. Ports connected to target servers or power strips are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of **Dominion-KX2_Port#** is assigned, where **Port#** is the number of the Dominion KX II physical port.

To change a port configuration:

1. Select **Device Settings > Port Configuration**. The Port Configuration Page opens:

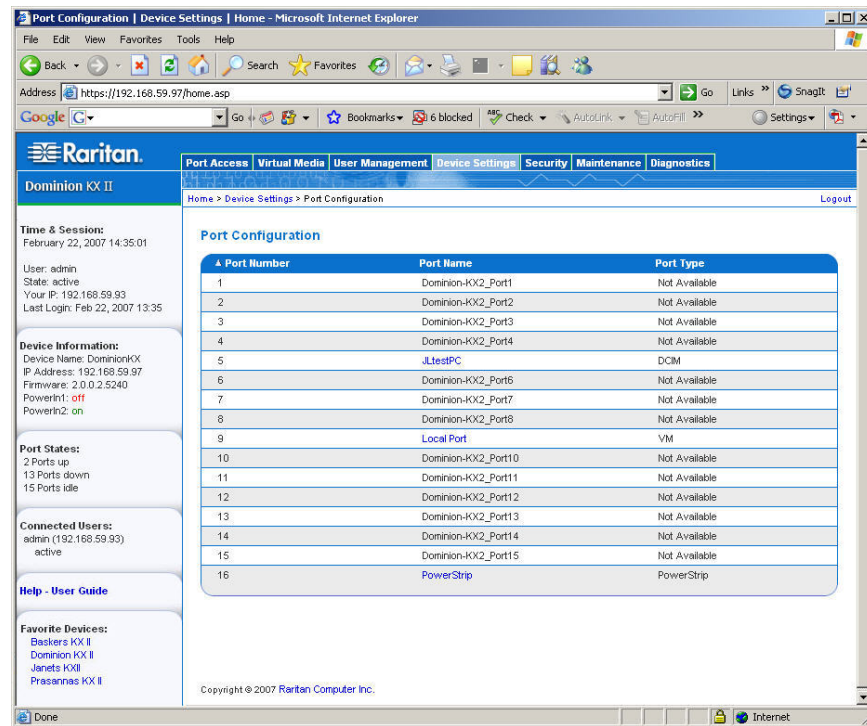


Figure 65: Port Configuration

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

- **Port Number.** Numbered from 1 to the total number of ports available for the Dominion KX II unit.
- **Port Name.** The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.
- **Port Type.** The type of CIM connected to the port:

PORT TYPE	DESCRIPTION
DCIM	Dominion CIM
Not Available	No CIM connected
PCIM	Paragon CIM
PowerStrip	Power CIM
VM	Virtual Media CIM (D2CIM-VUSB)

2. Click the **Port Name** for the port you want to edit.
 - For KVM ports, the [Port page](#) is opened. From this page, you can name the ports and create power associations.
 - For power strips, the Port page for [power strips](#) is opened. From this page, you can name the power strips and their outlets.

Power Control

The Dominion KX II provides remote power control of target servers. To utilize this feature, you must have a Raritan remote power strip and the D2CIM-PWR computer interface module (CIM). Once power assignments are made, remote power management of your target servers is possible.

To use the Dominion KX II power control feature:

1. [Connect the power strip](#) to your target server
2. [Name the power strip](#)
3. [Associate outlet\(s\)](#) in the power strip to the target server
4. Utilize remote [power management](#) of the target server from the [Port Access Page](#)

Connect the Power Strip

The numbers in this diagram correspond to the steps listed below.

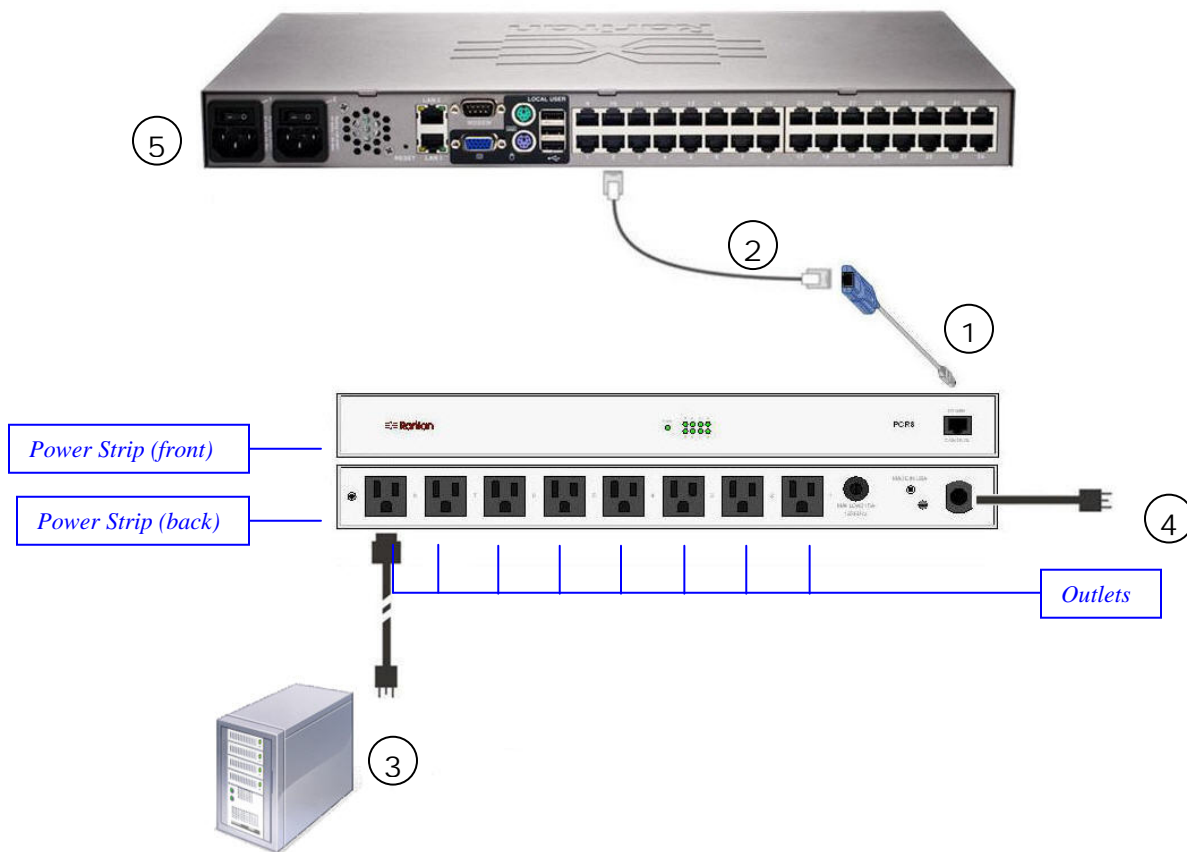


Figure 66: Power Strip Connections

To connect the power strip:

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector on the power strip.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the Dominion KX II using a straight through Cat 5 cable.
3. Attach an AC power cord to the target server and an available power strip outlet.
4. Connect the power strip to an AC power source.
5. Power ON the Dominion KX II unit.

Name the Power Strip (Port Page for Power Strips)

This Port page opens when you select a port from the [Port Configuration](#) page that is connected to a Raritan remote power strip. The **Type** and the **Name** fields are pre-populated; please note that the (CIM) **Type** *cannot* be changed. The following information is displayed for each outlet in the power strip: outlet **Number**, **Name**, and **Port Association**.

Use this page to name the power strip and its outlets; all names can be up to 32 alphanumeric characters and can include [special characters](#).

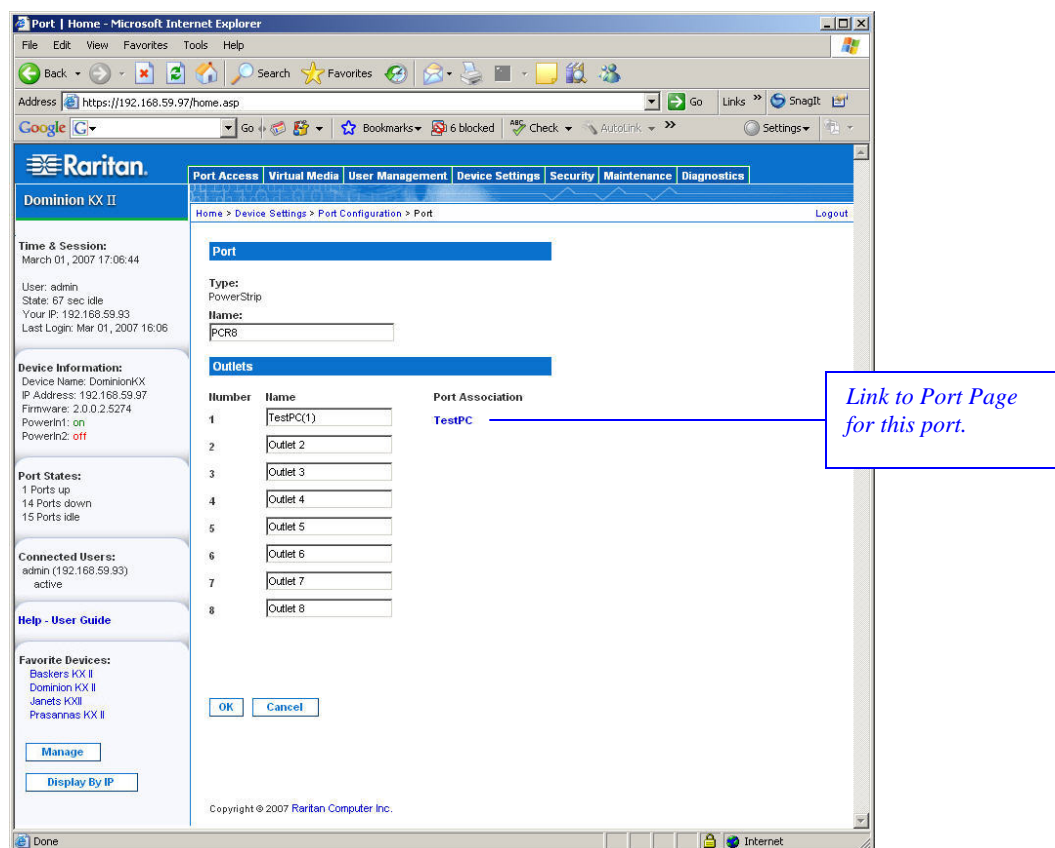


Figure 67: Port Page (power strips)

Note: When a power strip is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

To name the power strip (and outlets):

Note: CommandCenter Service Gateway does not recognize power strip names containing spaces.

1. Change the **Name** of the power strip to something you will remember.
2. Change the (Outlet) **Name** if desired. (Outlet names default to **Outlet #**.)
3. Click **OK**.

To cancel without saving changes:

Click the **Cancel** button.

Associate Target Servers to Outlets (Port Page)

This Port page opens when you select a port from the [Port Configuration](#) page that is connected to a target server. From this page, you can make power associations, change the Port Name to something more descriptive, and update target server settings if you are using the [D2CIM-VUSB CIM](#). The (CIM) **Type** and the (Port) **Name** fields are pre-populated; please note that the CIM type *cannot* be changed.

A server can have up to four power plugs and you can associate a different power strip with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote power strip(s)
- Power CIMs (D2CIM-PWR)

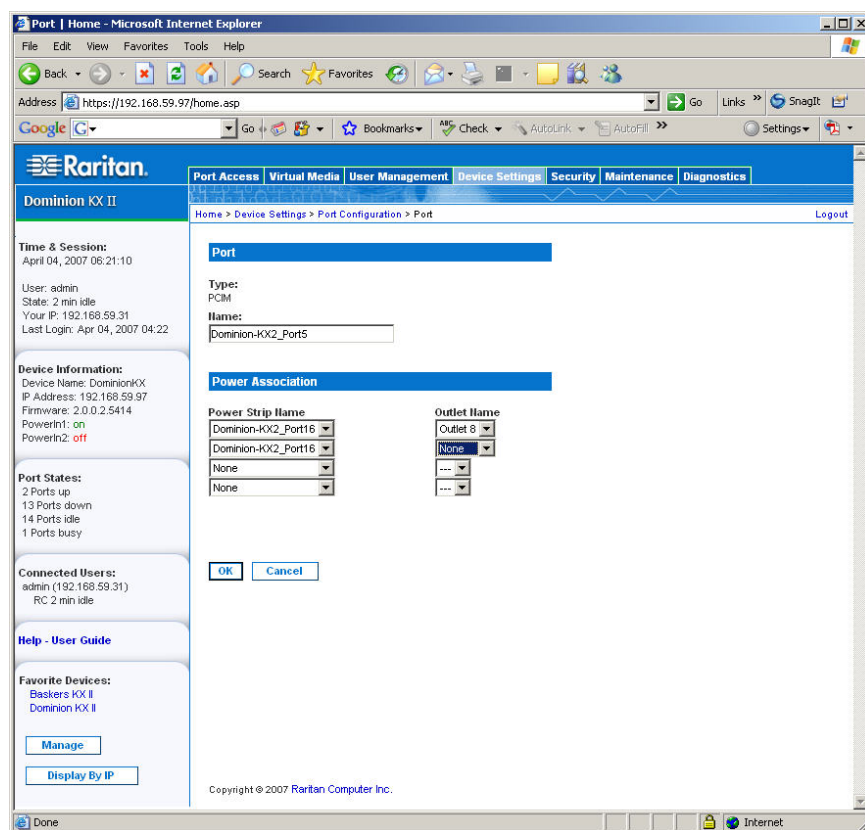


Figure 68: Port Page (KVM ports)

To make power associations (associate power strip outlets to target servers):

Note: When a power strip is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. Select the power strip from the **Power Strip Name** drop-down list.
2. For that power strip, select the outlet from the **Outlet Name** drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click **OK**. A confirmation message is displayed.

To change the port name:

1. Type something descriptive in the **Name** field. For example, the name of the target server would be a likely candidate. The name can be up to 32 alphanumeric characters and can include [special characters](#).
2. Click **OK**.

To cancel without saving changes:

Click the **Cancel** button.

To remove a power strip association:

1. Select the appropriate power strip from the **Power Strip Name** drop-down list.
2. For that power strip, select the appropriate outlet from the **Outlet Name** drop-down list.
3. From the **Outlet Name** drop-down list, select **None**.
4. Click **OK**. That power strip/outlet association is removed. A confirmation message is displayed.

Note for D2CIM-VUSB CIM Usage

If you are using the D2CIM-VUSB, there are additional settings on the Port page to improve performance.

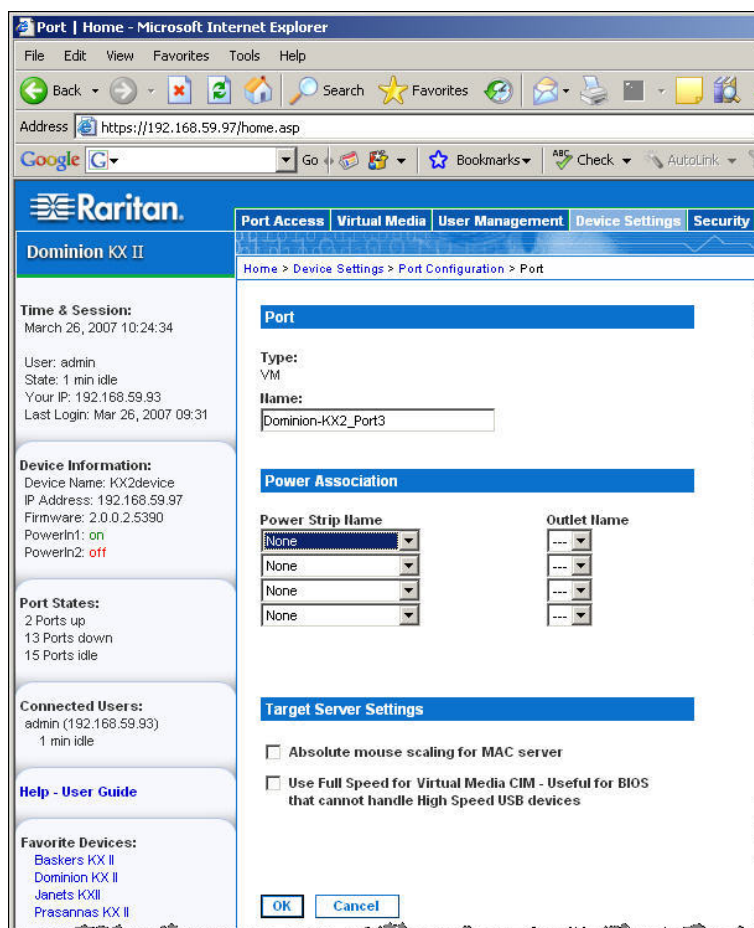


Figure 69: Port Page (Target Server Settings for D2CIM-VUSB)

If you are experiencing synchronization issues and are using the D2CIM-VUSB CIM for a Mac target server, check the **Absolute mouse scaling for MAC server** option.

Certain BIOS do not support USB high-speed capabilities and the attempt to auto-negotiate does not work. If you are experiencing BIOS problems with the target server, check the **Use Full Speed for Virtual Media CIM** option.

*Note: For SUSE 9.2 target servers, please enable (check) the **Use Full Speed for Virtual Media CIM** option for those target server ports. SUSE 9.2 does not work with the Virtual Media CIM when high speed is negotiated.*

Chapter 10: Security Settings

The Security menu is organized as follows: Security Settings and IP Access Control.

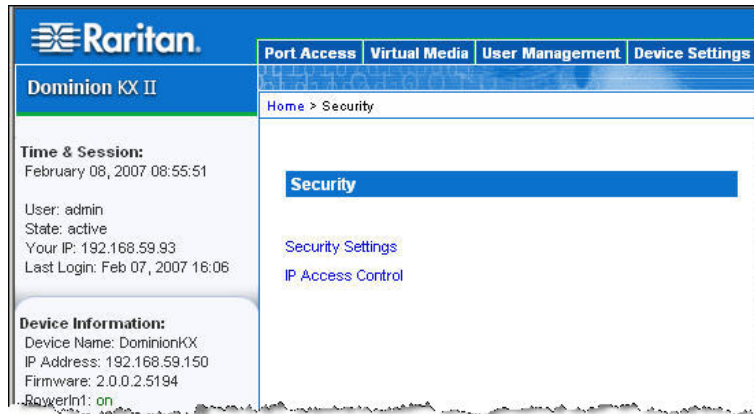


Figure 70: Security Menu

USE:	TO:
Security Settings	Configure security settings for login limitations, strong passwords, user blocking, and encryption & share.
IP Access Control	Control access to your Dominion KX II unit. By setting a global access control list, you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses.

Security Settings

From the Security Settings page, you can specify login limitations, user blocking, password rules, and encryption and share.

Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed; Java applet certificates are signed by a VeriSign® certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

To configure the security settings:

1. Select **Security > Security Settings**. The Security Settings page opens.

Figure 71: Security Settings

The fields are organized into the following groups: Login Limitations, Strong Passwords, User Blocking, and Encryption & Share.

2. Update the [Login Limitations](#) settings as appropriate.
3. Update the [Strong Passwords](#) settings as appropriate.
4. Update the [User Blocking](#) settings as appropriate.
5. Update the [Encryption & Share](#) settings as appropriate.
6. Click **OK** when you are done.

To close the page without saving any changes:

Click **Cancel**.

To reset back to defaults:

Click **Reset to Defaults**.

Login Limitations

Using Login Limitations you can specify restrictions for single login, password aging, and the logging out of idle users.

- **Enable Single Login Limitation.** When checked, only one login per username is allowed at any time. When cleared, a given username/password combination can be connected into the device from several client workstations simultaneously.
- **Enable Password Aging.** When checked, all users are required to change their passwords periodically, based on the number of days specified in **Password Aging Interval** field.
 - **Password Aging Interval (days).** This field is enabled and required when the **Enable Password Aging** checkbox is checked. Enter the number of days after which a password change is required. The default is 60 days.
- **Log Out Idle Users.** Check the checkbox to automatically disconnect a user session after a certain amount of inactive time has passed. Type the amount of time in the **After** field. If there is no activity from the keyboard or mouse, all KVM sessions and all KVM resources are logged out. If a Virtual Media session is in progress, however, the session does not timeout.
 - **After (minutes).** The amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the **Log Out Idle Users** option is checked.

Strong Passwords

Strong passwords provide more secure local authentication for the system. Using Strong Passwords, you can specify criteria defining the format of valid KX II local passwords such as minimum and maximum length, required characters, and password history retention.

Figure 72: Security Settings (Strong Passwords)

- **Enable strong passwords.** Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one non-alphabetical character (punctuation character or number). In addition, the first four characters of the password and the username cannot match.

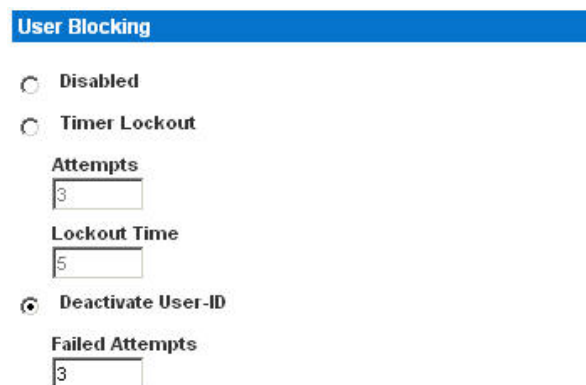
When checked, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When cleared, only the standard format validation is enforced. When checked, the following fields are enabled and required:

- **Minimum length of strong password.** Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
- **Maximum length of strong password.** The default is 16, but can be up to 64 characters long.
- **Enforce at least one lower case character.** When checked, at least one lower case character is required in the password.
- **Enforce at least one upper case character.** When checked, at least one upper case character is required in the password.
- **Enforce at least one numeric character.** When checked, at least one numeric character is required in the password.
- **Enforce at least one printable special character.** When checked, at least one special character (printable) is required in the password.
- **Number of restricted passwords based on history.** This field represents the password history depth; that is, the number of prior passwords that cannot be repeated. The range is 1-12; the default is 5.

User Blocking

The User Blocking options specify the criteria in which users are blocked from accessing the system after the specified number of unsuccessful login attempts. The three options are mutually exclusive:

- **Disabled.** The default option; users are not blocked regardless of the number of times they fail authentication.
- **Timer Lockout.** Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:
 - **Attempts.** The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 – 10; the default is 3 attempts.
 - **Lockout Time.** The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes; the default is 5 minutes.
- **Deactivate User-ID.** When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the **Failed Attempts** field:
 - **Failed Attempts.** The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the **Deactivate User-ID** option is selected. The valid range is 1 - 10.



User Blocking

☐ Disabled

☐ Timer Lockout

Attempts
3

Lockout Time
5

☒ Deactivate User-ID

Failed Attempts
3

Figure 73: Security Settings (User Blocking)

When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by checking the **Active** checkbox in the [User](#) page.

Encryption & Share

Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the Dominion KX II reset button is pressed.

Encryption & Share

Encryption Mode
Auto

☒ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
Private

☐ VM Share Mode

Local Device Reset Mode
Enable Local Factory Reset

Figure 74: Security Settings (Encryption & Share)

- **Encryption Mode.** Select one of the options from the drop-down list. When an encryption mode is selected, a warning is displayed that if your browser does not support the selected mode, you will not be able to connect to the Dominion KX II:

Encryption & Share

When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the Dominion KX II.

Encryption Mode
RC4

☒ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
Private

☐ VM Share Mode

Local Device Reset Mode
Enable Local Factory Reset

Figure 75: Security Settings (Encryption Mode Warning Message)

- **Auto.** This is the recommended option; the Dominion KX II auto-negotiates to the highest level of encryption possible.
- **RC4.** Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol which provides a private communications channel between the Dominion KX II unit and the Remote PC during initial connection authentication.
- **AES-128.** The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 128 is the key length. When AES-128 is specified, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to [Checking Your Browser for AES Encryption](#) for more information.
- **Apply Encryption Mode to KVM and Virtual Media.** When checked, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.

- **PC Share Mode.** Determines *global* concurrent remote KVM access, enabling up to eight remote users to simultaneously log on to one Dominion KX II and concurrently view and control the same target server through the device. Click on the drop-down list to select one of the following options:
 - **Private:** No PC share; this is the default mode. Each target server can be *accessed exclusively* by only one user at a time.
 - **PC-Share:** Target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, please note that uneven control will occur if one user does not stop typing or moving the mouse.
- **VM Share Mode.** This option is enabled only when **PC-Share Mode** is enabled. When checked, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.
- **Local Device Reset Mode.** This option specifies which actions are taken when the hardware reset button (at the back of the unit) is depressed. For more information, refer to [Reset Button](#). Select one of the following options:
 - **Enable Local Factory Reset** (Default). Returns the Dominion KX II unit to the factory defaults.
 - **Enable Local Admin Password Reset.** Resets the local administrator password only. The password is reset to **raritan**.
 - **Disable All Local Resets.** No reset action is taken.

Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer, or navigate to the following web site using the browser with the encryption method you want to check: <https://www.fortify.net/sslcheck.html>. This web site detects your browser's encryption method and displays a report.

IP Access Control

Using IP Access Control, you can control access to your Dominion KX II unit. By setting a global Access Control List (ACL) you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP Access Control is global, affecting the KX unit as a whole, but you can also control access to your unit at the group level. Refer to [group-based IP Access Control](#) for more information about group-level control.

Important: IP Address 127.0.0.1 is used by the Dominion KX II local port. When creating an IP Access Control list, if 127.0.0.1 is within the range of IP Addresses that are blocked, you will not have access to the Dominion KX II local port.

To use IP Access Control:

1. Open the IP Access Control page using one of these methods:

- Select **Security > IP Access Control**, or
- Click the **Set System ACL** button from the [Network Settings](#) page

The IP Access Control page opens:

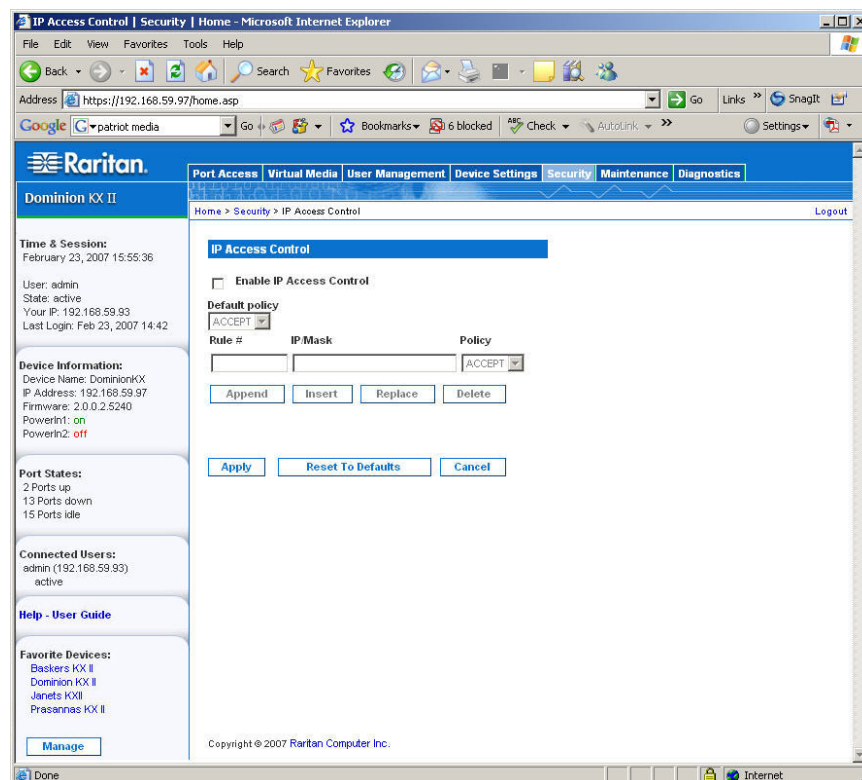


Figure 76: IP Access Control

2. Check the **Enable IP Access Control** checkbox to enable IP access control and the remaining fields on the page.
3. Select the **Default Policy**. This is the action taken for IP addresses that are not within the ranges you specify.
 - **Accept.** IP Addresses are allowed access to the Dominion KX II device.
 - **Drop.** IP Addresses are denied access to the Dominion KX II device.

To add (append) rules:

1. Type the IP Address and subnet mask in the **IP/Mask** field.
2. Select the **Policy** from the drop-down list.
3. Click **Append**. The rule is added to the bottom of the rules list.
4. Repeat steps 1 through 3 for each rule you want to enter.

To insert a rule:

1. Type a **Rule #**. A Rule # is required when using the Insert command.
2. Type the IP Address and subnet mask in the **IP/Mask** field.
3. Select the **Policy** from the drop-down list.
4. Click **Insert**. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

To replace a rule:

1. Specify the **Rule #** you want to replace.
2. Type the IP Address and subnet mask in the **IP/Mask** field.
3. Select the **Policy** from the drop-down list.
4. Click **Replace**. Your new rule replaces the original rule with the same Rule #.

To delete a rule:

1. Specify the **Rule #** you want to delete.
2. Click **Delete**.
3. You are prompted to confirm the deletion. Click **OK**.

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

Chapter 11: Maintenance

The Maintenance menu includes these options: Audit Log, Device Information, Backup/Restore, CIM Firmware Upgrade, Firmware Upgrade, Factory Reset (Dominion KX II Local Console only), Upgrade Report, and Reboot.

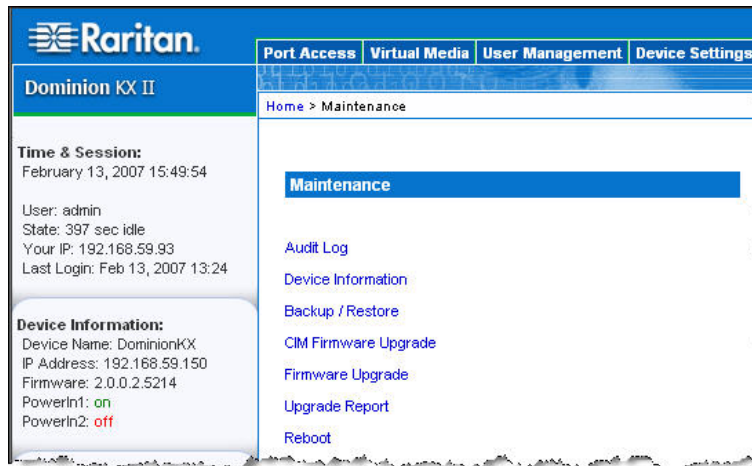


Figure 77: Maintenance Menu

USE:	To:	LOCAL	REMOTE
Audit Log	View Dominion KX II events sorted by date and time.	✓	✓
Device Information	View information about the Dominion KX II and its CIMs.	✓	✓
Backup/Restore	Backup and restore the KX II configuration.		✓
CIM Firmware Upgrade	Upgrade your CIMs using the firmware versions stored in the Dominion KX II memory.	✓	✓
Firmware Upgrade	Upgrade your Dominion KX II firmware.		✓
Factory Reset	Perform a factory reset.	✓	
Upgrade Report	View information about the latest upgrade performed.	✓	✓
Reboot	Reboot the Dominion KX II unit.	✓	✓

Audit Log

A log is created of Dominion KX II system events.

To view the audit log for your Dominion KX II unit:

Select **Maintenance > Audit Log**. The Audit Log page opens:

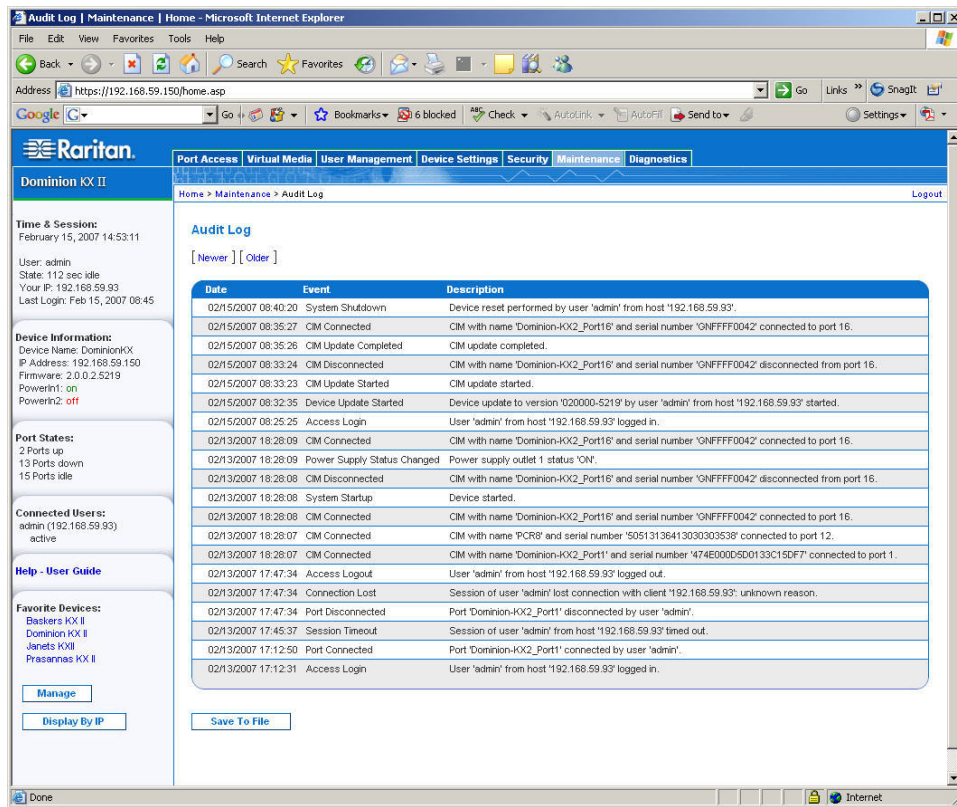


Figure 78: Audit Log

The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

- **Date.** The date and time that the event occurred; 24-hour clock.
- **Event.** The event name as listed in the Event Management page.
- **Description.** Detailed description of the event.

To save the Audit Log:

Note: Saving the Audit Log is available only on the Dominion KX II Remote Console, not on the Local Console.

1. Click the **Save to File** button. A Save File dialog opens.
2. Select the desired file name and location and click **Save**. The audit log is saved *locally* on your client machine with the name and location specified.

To page through the Audit Log:

Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your Dominion KX II device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

To view information about your Dominion KX II and CIMs:

Select **Maintenance > Device Information**. The Device Information page opens:

The screenshot shows the Raritan Dominion KX II web interface. The browser window title is "Device Information | Maintenance | Home - Microsoft Internet Explorer". The address bar shows "https://192.168.59.97/home.asp". The page has a blue header with the Raritan logo and navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance, and Diagnostics. The "Maintenance" tab is selected, and the "Device Information" sub-tab is active. The page content is divided into several sections:

- Time & Session:** April 09, 2007 10:44:47; User: admin; State: 1 min idle; Your IP: 192.168.59.41; Last Login: Apr 09, 2007 09:53.
- Device Information:** Device Name: DominionKX; IP Address: 192.168.59.97; Firmware: 2.0.0.2.5418; PowerIn1: on; PowerIn2: off.
- Port States:** 2 Ports up; 13 Ports down; 15 Ports idle.
- Connected Users:** admin (192.168.59.41); 1 min idle.
- Help - User Guide** link.
- Favorite Devices:** Baskers KX II, Dominion KX II, with "Manage" and "Display By IP" buttons.
- Device Information (Summary):**
 - Model: DKX2-416
 - Hardware Revision: 0x44
 - Firmware Version: 2.0.0.2.5418
 - Serial Number: HKC6B00016
 - MAC Address: 00:0d:5d:01:33:c1
- CIM Information Table:**

Port	Name	Type	Firmware Version	Serial Number
1	Dominion-KX2_Port1	VM	2A36	HUM7250771
3	Dominion-KX2_Port3	PCIM	N/A	GNFFFFFFFFFFFF7565
8	Dominion-KX2_Port8	PowerStrip	00B2	PQ16A00058

At the bottom, there is a copyright notice: "Copyright © 2007 Raritan Computer Inc." and a status bar showing "Done" and "Internet".

Figure 79: Device Information

The following information is provided about the Dominion KX II: **Model**, **Hardware Revision**, **Firmware Version**, **Serial Number**, and **MAC Address**.

The following information is provided about the CIMs in use: **Port** (number), **Name**, **Type** (of CIM: DCIM, PCIM, Power Strip, or VM), **Firmware Version**, and **Serial Number**.

Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your Dominion KX II. In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism. For instance, you can quickly provide access to your team from another Dominion KX II, by backing up the user configuration settings from the KX II in use and restoring those configurations to the new KX II. You can also setup one Dominion KX II and copy its configuration to multiple KX II devices.

To access the Backup/Restore page:

Select **Maintenance > Backup/Restore**. The Backup/Restore page opens:

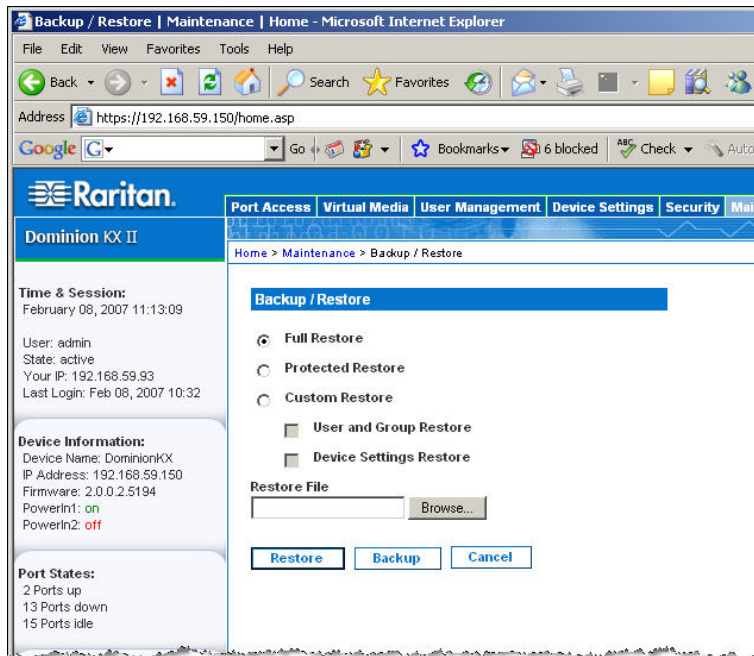


Figure 80: Backup/Restore

Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

To backup your Dominion KX II:

1. Click **Backup**. A File Download dialog opens.
2. Click **Save**. A Save As dialog opens.
3. Select the location, specify a file name, and click **Save**. A Download Complete dialog opens.
4. Click **Close**. The backup file is saved *locally* on your client machine with the name and location specified.

To restore your Dominion KX II:

WARNING: Please exercise caution when restoring your Dominion KX II to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the KX II.

In addition, if you used a different IP Address at the time of the backup, that IP Address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Select the type of restore you want to run:
 - **Full Restore.** A complete restore of the entire system; generally used for traditional backup and restore purposes.
 - **Protected Restore.** Everything is restored *except* device-specific information such as serial number, MAC Address, IP Address, name, port names, etc. With this option, you can setup one Dominion KX II and copy the configuration to multiple KX II devices.
 - **Custom Restore.** With this option, you can select **User and Group Restore**, **Device Settings Restore**, or both. Check the appropriate checkboxes:
 - **User and Group Restore.** This option includes only user and group information. Use this option to quickly setup users on a different Dominion KX II.
 - **Device Settings Restore.** This option includes only device settings. Use this option to quickly copy the device information.
2. Click the **Browse** button. A Choose file dialog opens.
3. Navigate to and select the appropriate backup file and click **Open**. The file selected is listed in the **Restore File** field.
4. Click **Restore**. The configuration (based on the type of restore selected) is restored.

CIM Upgrade

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your Dominion KX II unit. In general, all CIMs are upgraded when you upgrade the device firmware using the [Firmware Upgrade](#) page. Use the CIM Upgrade page to upgrade new CIMs.

Note: Only D2CIM-VUSB and D2CIM-PWR can be upgraded from this page.

To upgrade CIMs using the Dominion KX II memory:

1. Select **Maintenance > CIM Firmware Upgrade**. The CIM Upgrade from KX Flash page opens:

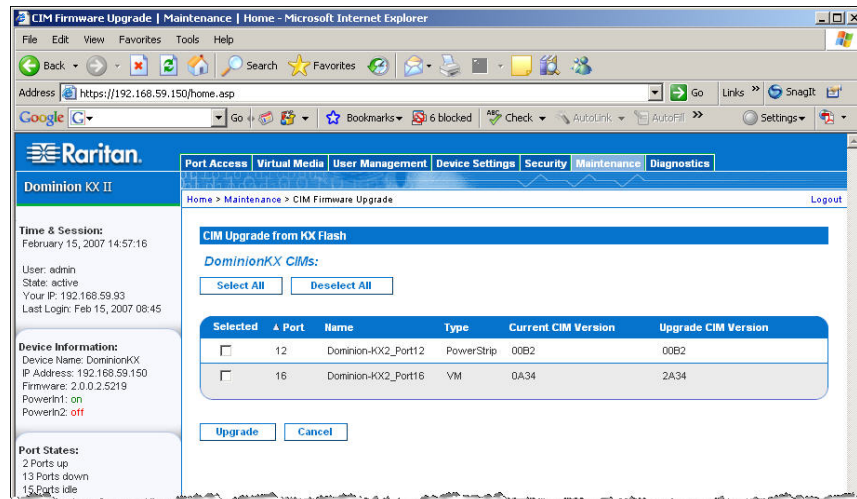


Figure 81: CIM Upgrade from KX Flash

2. The **Port** (number), **Name**, **Type**, **Current CIM Version**, and **Upgrade CIM Version** are displayed for easy identification of the CIMs.
3. Check the **Selected** checkbox for each CIM you want to upgrade.

Tip: Use the **Select All** and **Deselect All** buttons to quickly select all (or deselect all) of the CIMs.

4. Click the **Upgrade** button. You are prompted to confirm the upgrade.
5. Click **OK** to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes (or less) per CIM.

To exit without upgrading:

Click the **Cancel** button.

Firmware Upgrade

Use the Firmware Upgrade page to upgrade the firmware for your Dominion KX II unit and all attached CIMs. This page is available in the *KX II Remote Console only*.

Important: Do not turn off your Dominion KX II unit or disconnect CIMs while the upgrade is in progress – doing so will likely result in damage to the unit or CIMs.

To upgrade your Dominion KX II unit:

1. Locate the appropriate Raritan firmware distribution file (*.RFP), found on the Raritan Firmware Upgrades Web page: <http://www.raritan.com/support/firmwareupgrades> and download the file.
2. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

3. Select **Maintenance > Firmware Upgrade**. The Firmware Upgrade page opens:

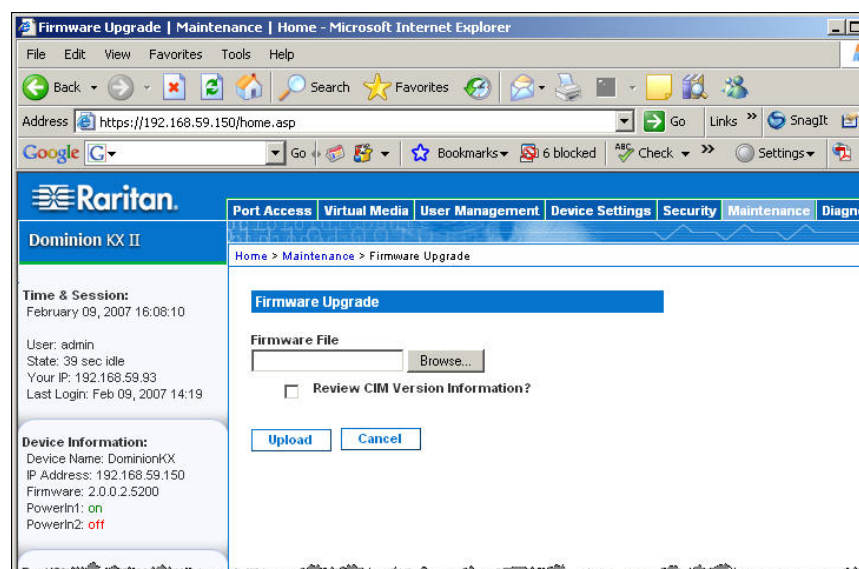


Figure 82: Firmware Upgrade

4. Click the **Browse** button to navigate to the directory where you unzipped the upgrade file.
5. Check the **Review CIM Version Information?** checkbox if you would like information displayed about the versions of the CIMs in use.
6. Click **Upload** from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review CIM information, that information is displayed as well):

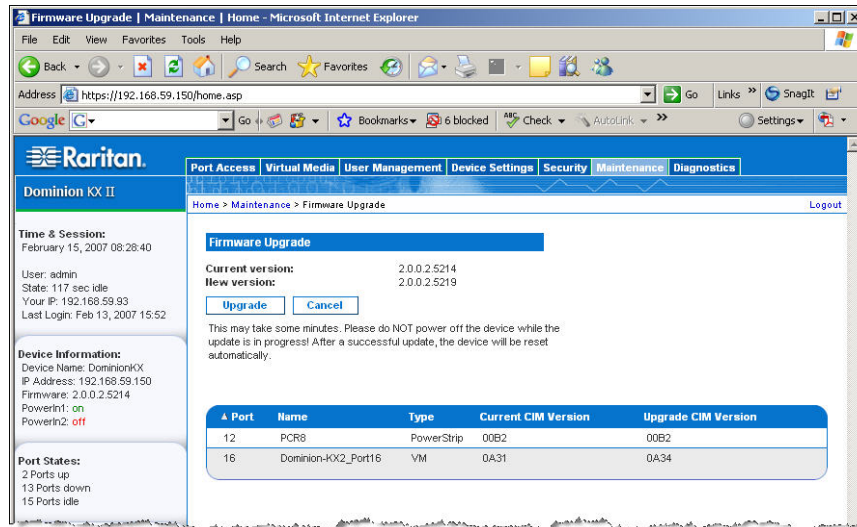


Figure 83: Firmware Upgrade Review

Note: At this point, connected users are logged out, and new login attempts are blocked.

- Click **Upgrade**. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the unit reboots (1 beep sounds to signal the reboot).

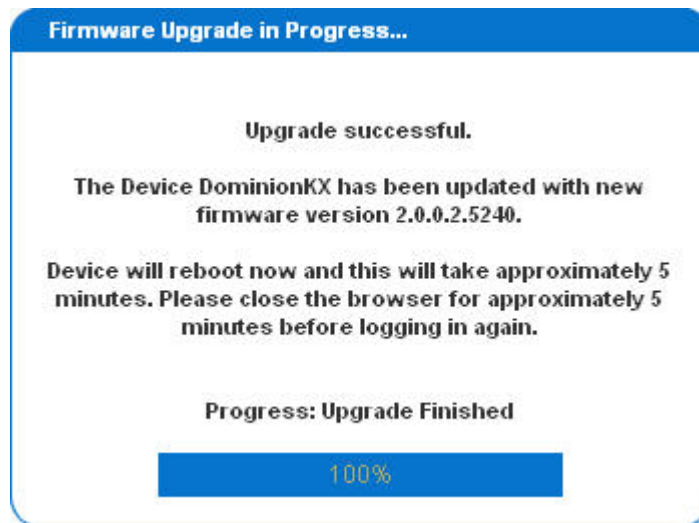


Figure 84: Firmware Upgrade Successful

- As prompted, close the browser and wait approximately 5 minutes before logging in to the Dominion KX II again.

For information about upgrading the device firmware using the Multi-Platform Client, refer to the *Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide*.

Upgrade Report

Dominion KX II provides information about upgrades performed on the KX II unit and attached CIMS.

To view the upgrade report:

Select **Maintenance > Upgrade Report**. The Upgrade Report page opens:

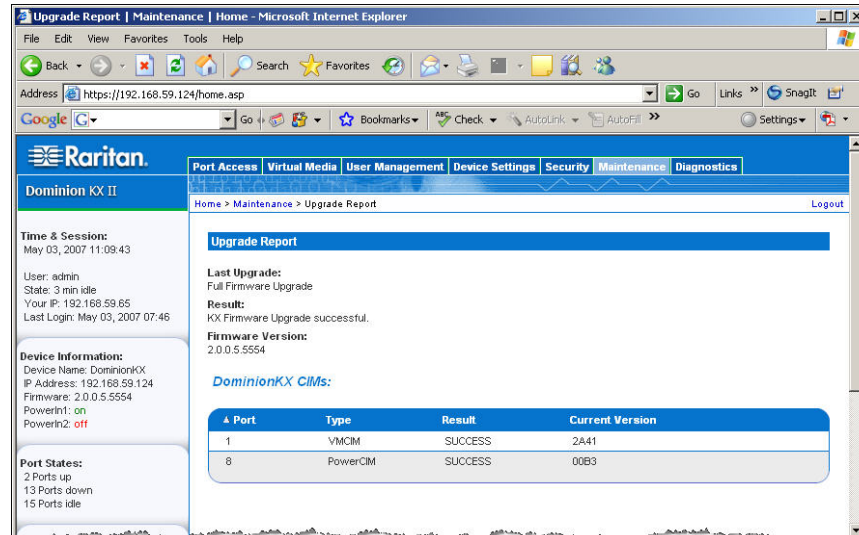


Figure 85: Upgrade Report

Information is provided about the last Dominion KX II upgrade that was run, the final status of that upgrade, and the firmware version. Information is also provided about the CIMs:

- **Port.** The port where the CIM is connected.
- **Type.** The type of CIM.
- **Result.** The result of the upgrade (success or fail).
- **Current Version.** The CIM firmware version.

Reboot

The Reboot page provides a safe and controlled way to reboot your Dominion KX II unit; this is the recommended method for rebooting.

Important: All KVM connections will be closed and all users will be logged off.

To reboot your Dominion KX II:

1. Select **Maintenance > Reboot**. The Reboot page opens:

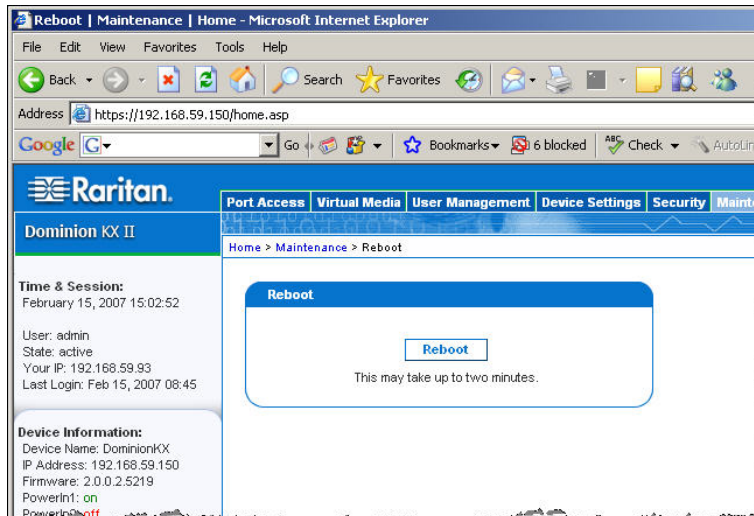


Figure 86: Reboot

2. Click the **Reboot** button. You are prompted to confirm the action:

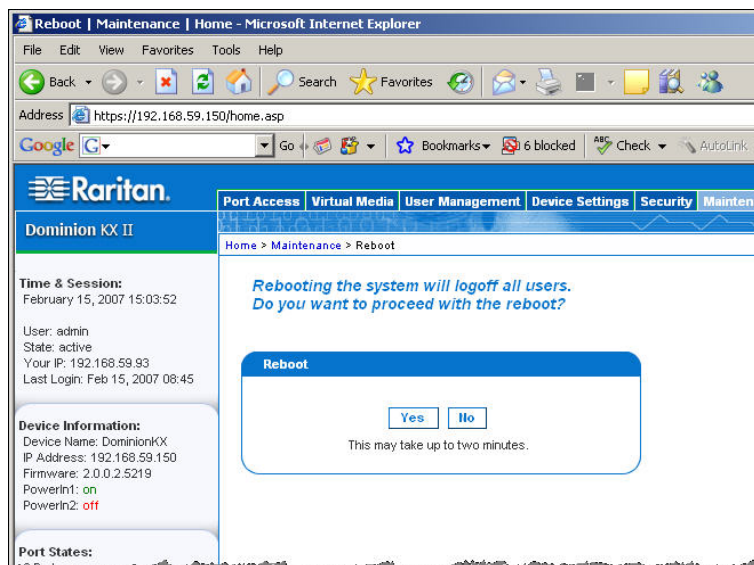


Figure 87: Reboot Confirmation

3. Click **Yes** to proceed with the reboot.

To exit without rebooting:

Click **No**.

Chapter 12: Diagnostics

Diagnostics Menu

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the KX II device. All of the Diagnostics pages (except KX Diagnostics) run standard networking commands; the information displayed is the output of those commands.

The following Diagnostics menu options help you debug and configure the network settings:

- Network Interface
- Network Statistics
- Ping Host
- Trace Route to Host

The KX Diagnostics option is intended for use in conjunction with Raritan Technical Support.

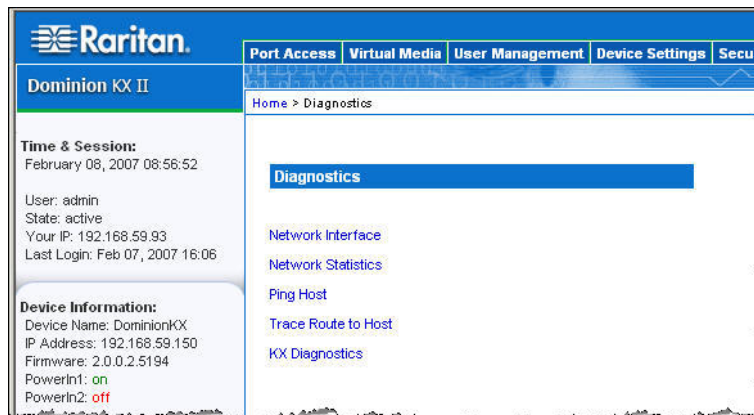


Figure 88: Diagnostics Menu

USE:	TO:
Network Interface	Obtain the status of network interface.
Network Statistics	Obtain statistics about the network.
Ping Host	Determine whether a particular host is reachable across an IP network.
Trace Route to Host	Determine the route taken all the way to the selected host.
KX Diagnostics	Use when directed by Raritan Technical Support (<i>Remote Console only</i>).

Network Interface Page

The Dominion KX II provides information about the status of your network interface.

To view information about your network interface:

Select **Diagnostics > Network Interface**. The Network Interface page opens:

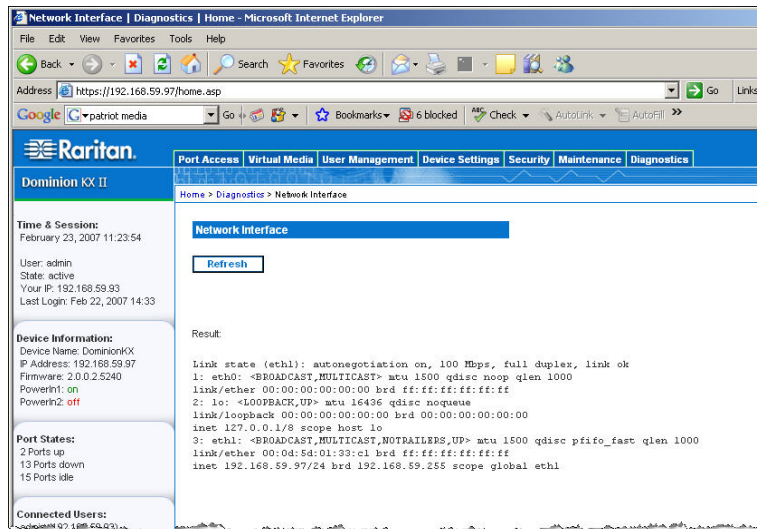


Figure 89: Network Interface

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is ping-able or not.
- The LAN port that is currently active.

To refresh this information:

Click the **Refresh** button.

Network Statistics Page

The Dominion KX II provides statistics about your network interface.

To view statistics about your network interface:

1. Select **Diagnostics > Network Statistics**. The Network Statistics page opens.
2. Select the appropriate option from the **Options** drop-down list:
 - **Statistics**. Produces a page similar to the one displayed here:

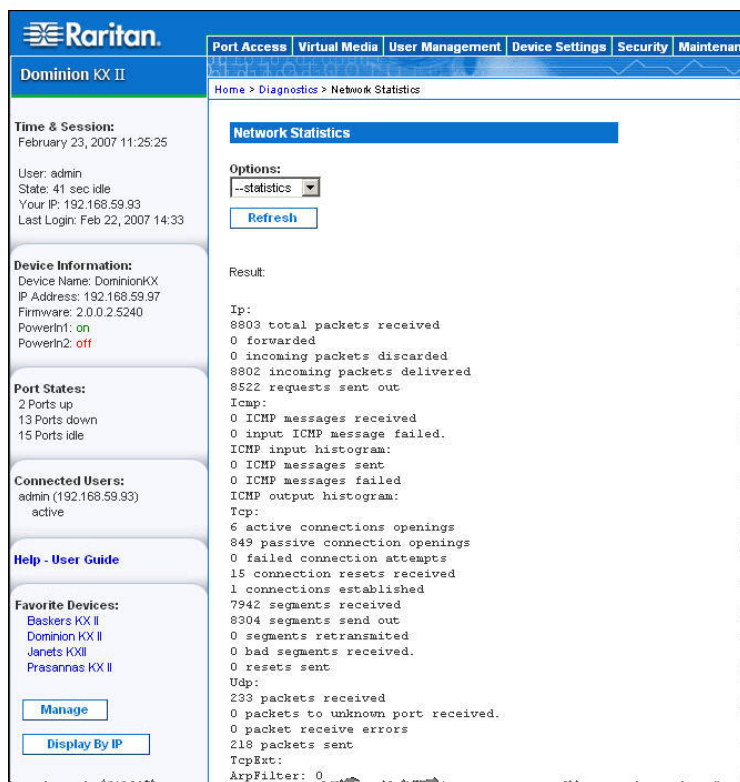


Figure 90: Network Statistics (statistics)

- **Interfaces**. Produces a page similar to the one displayed here:

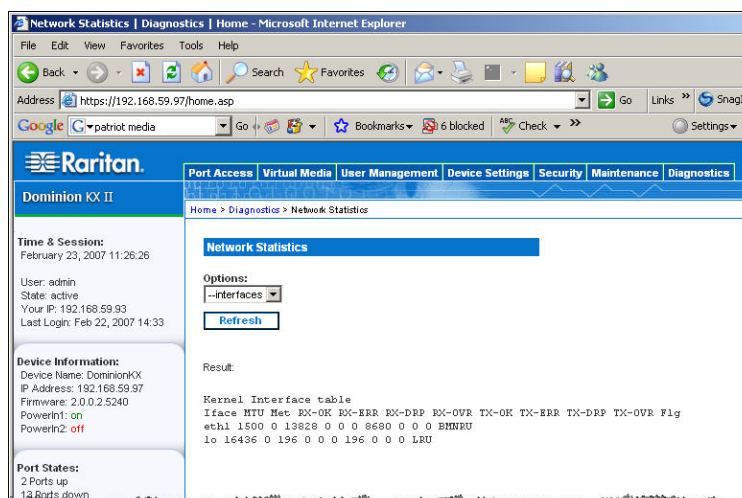


Figure 91: Network Statistics (interfaces)

- **Route**. Produces a page similar to the one displayed here:

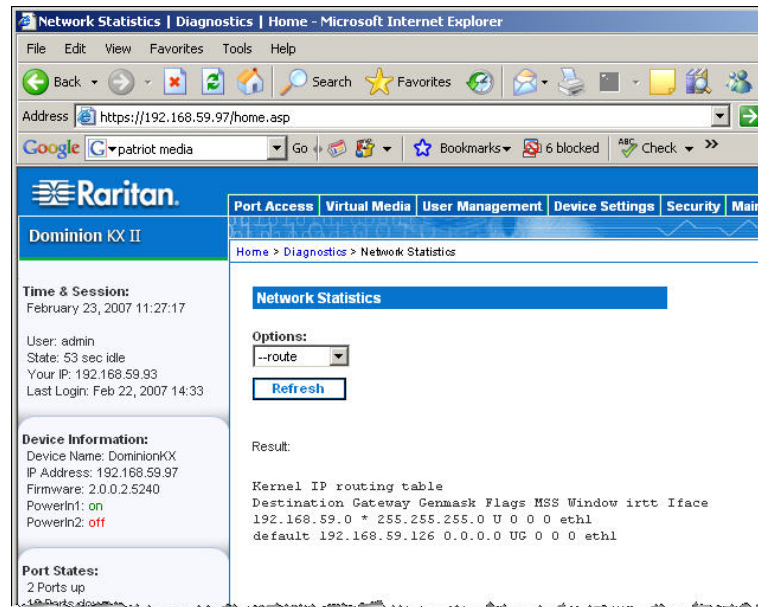


Figure 92: Network Statistics (route)

3. Click the **Refresh** button.

The relevant information is displayed in the **Result** field.

Ping Host Page

Ping is a network tool used to test whether a particular host or IP Address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another Dominion KX II unit is accessible.

To ping the host:

1. Select **Diagnostics > Ping Host**. The Ping Host page opens:

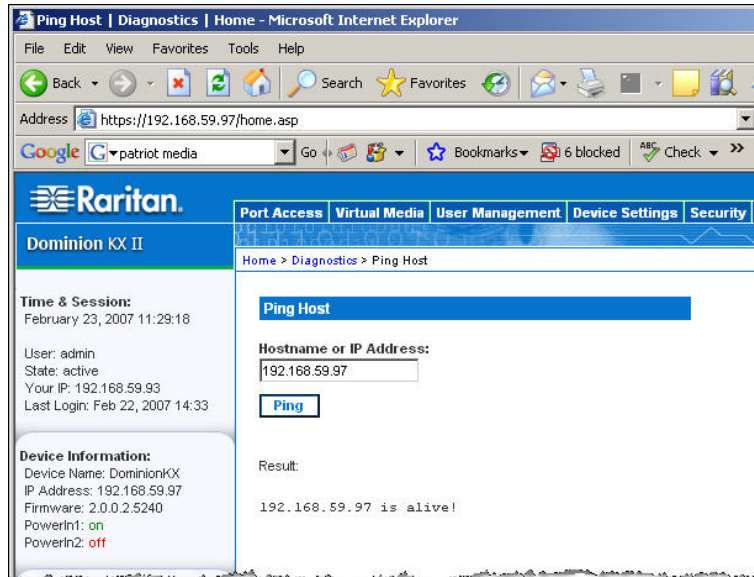


Figure 93: Ping Host

2. Type either the hostname or IP Address into the **Hostname or IP Address** field.
3. Click **Ping**. The results of the ping are displayed in the **Result** field.

Trace Route to Host Page

Trace route is a network tool used to determine the route taken all the way to the provided hostname or IP Address.

To trace the route to the host:

1. Select **Diagnostics > Trace Route to Host**. The Trace Route to Host page opens:

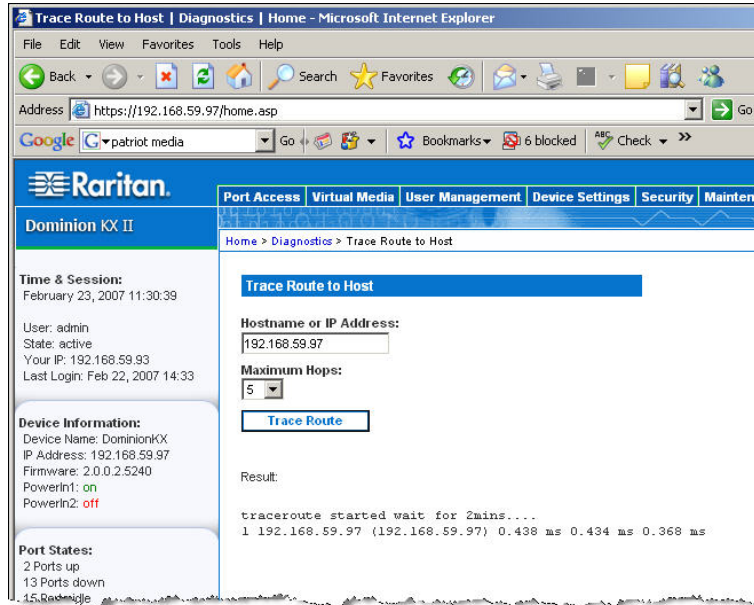


Figure 94: Trace Route to Host

2. Type either the Hostname or IP Address into the **Hostname or IP Address** field.
3. Select the **Maximum Hops** from the drop-down list (5 or 10).
4. Click the **Trace Route** button. The trace route command is executed for the given hostname or IP Address and the maximum hops. The output of trace route is displayed in the **Result** field.

KX Diagnostics

Note: This page is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

KX Diagnostics downloads the diagnostics information from Dominion KX II to the client machine. Three operations can be performed on this page:

- **Command Line Interface.** Enable or disable the Command Line Interface functionality. With this feature, a Raritan Technical Support engineer can open a standard SSH client, connect to the unit, and remotely execute diagnostic functions.
- **Diagnostics Scripts.** Execute a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the unit and executed. Once this script has been executed, you can download the diagnostics messages through the **Save to File** button.
- **KX Diagnostic Log.** Download the snapshot of diagnostics messages from the KX II unit to the client. This encrypted file is then sent to Raritan Technical Support; only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

To run the KX II System diagnostics:

1. Select **Diagnostics > KX Diagnostics**. The KX Diagnostics page opens.

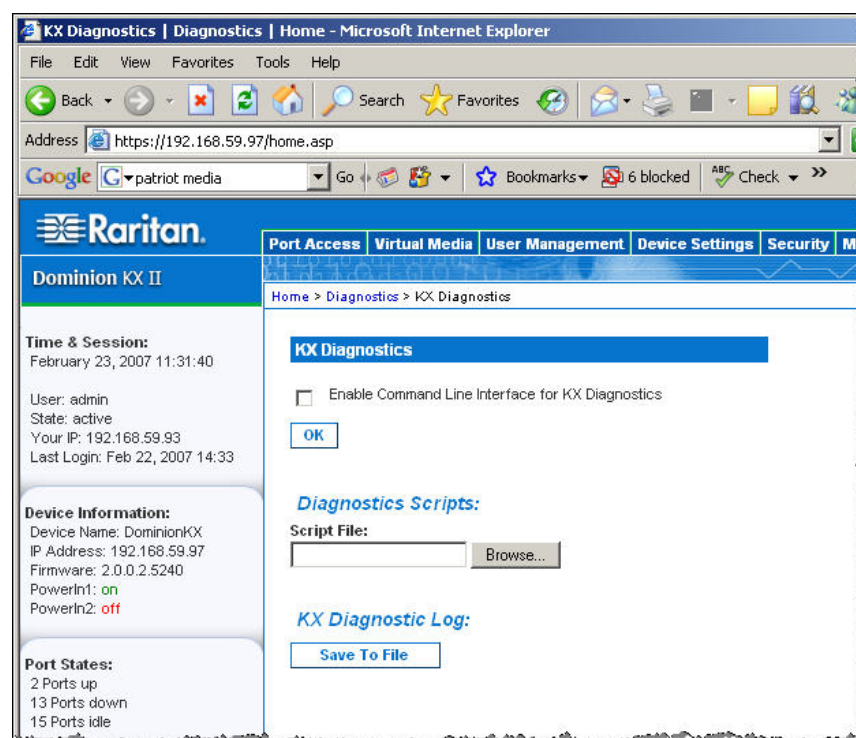


Figure 95: KX Diagnostics

2. To enable the Command Line Interface for use by Raritan Technical Support:

Note: UDP Port 21 is required for this feature.

- a. Check the **Enable Command Line Interface for KX Diagnostics** checkbox.
- b. Click **OK**.

- c. UDP port 21 must be opened and made available to Raritan Technical Support.
 - d. Raritan Technical Support will also need to know the administrative password for the KX II.
 - e. Once Raritan Technical Support has completed their testing, return UDP port 21 to its original state.
3. To execute a diagnostics script file emailed to you from Raritan Technical Support:
 - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
 - b. Use the **Browse** button. A Choose file dialog opens.
 - c. Navigate to and select this diagnostics file.
 - d. Click **Open**. The file is displayed in the **Script File** field:



Figure 96: Diagnostics Scripts

- e. Click **Run Script**.
 - f. Sent this file to Raritan Technical Support using step 4.
4. To create a diagnostics file to send to Raritan Technical Support:
 - a. Click the **Save to File** button. The File Download dialog opens:

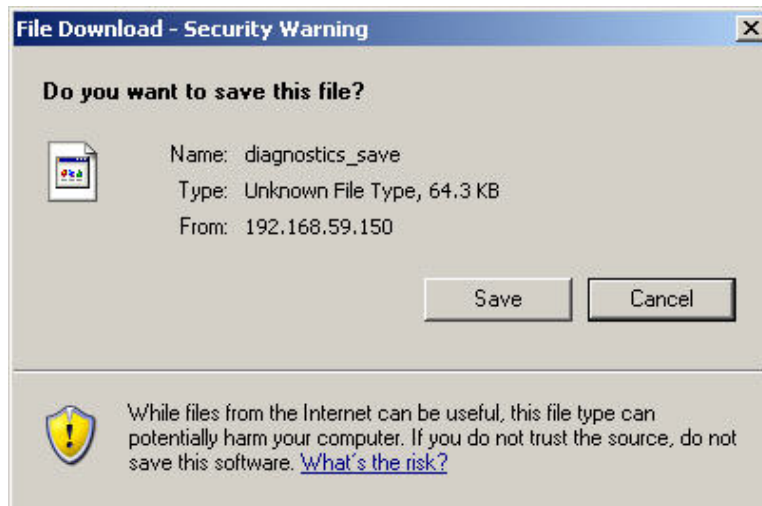


Figure 97: File Download

- b. Click **Save**. The Save As dialog opens.
 - c. Navigate to the desired directory and click **Save**.
 - d. Email this file as directed by Raritan Technical Support.

Chapter 13: KX II Local Console

KX II Local Console

Dominion KX II provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The Dominion KX II Local Console provides a direct analog connection to your connected servers; the performance is as if you were directly connected to the server's keyboard, mouse, and video ports. The KX II Local Console provides the same administrative functionality as the Dominion KX II Remote Console.

The Dominion KX II Local Console supports the following language keyboards: US English, UK English, German, French, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Note: Keyboard use for Chinese, Japanese, and Korean is for display only; local language input is not supported at this time for KX II Local Console functions.

The screenshot displays the Dominion KX II Local Console web interface. The top navigation bar includes links for Port Access, User Management, Device Settings (selected), Security, Maintenance, and Diagnostics. The main content area is divided into two columns. The left column shows system status: Time & Session (May 02, 2007 10:06:59), User (admin), State (36 min idle), Your IP (Local Console), Last Login (May 02, 2007 04:11), Device Information (Device Name: DominionKX, IP Address: 192.168.59.124, Firmware: 2.0.0.5.5541, PowerIn1: on, PowerIn2: off), Port States (2 Ports up, 13 Ports down, 14 Ports idle, 1 Ports busy), and Connected Users (admin (Local Console), 36 min idle; admin (192.168.59.65), RC active). The right column contains two settings panels. The 'Network Basic Settings' panel includes fields for Device Name (DominionKX), IP auto configuration (DHCP), Preferred host name (DHCP only), IP address (192.168.59.124), Subnet mask (255.255.255.0), Gateway IP address (192.168.59.126), Primary DNS server IP address (192.168.59.2), and Secondary DNS server IP address (192.168.51.10). The 'Network Miscellaneous Settings' panel includes Discovery Port (5000), Bandwidth Limit (No Limit), LAN Interface Settings (Autodetect), and a note about reliable network communication. Below these panels are buttons for OK, Reset to defaults, and Cancel.

Figure 98: Dominion KX II Local Console

Physical Connections

The physical connections for the local ports can be found on the back panel of the Dominion KX II:



Figure 99: Local User Panel on Dominion KX II

Monitor: Attach a standard multi-sync VGA monitor to the HD15 (female) video port.

Keyboard: Attach *either* a standard PS/2 keyboard to the Mini-DIN6 (female) keyboard port, *or* a standard USB keyboard to one of the USB Type A (female) ports.

Mouse: Attach *either* a standard PS/2 mouse to the Mini-DIN6 (female) mouse port *or* a standard USB mouse to one of the USB Type A (female) ports.

Reset Button

At the back of the Dominion KX II unit, there is a Reset button. It is recessed to prevent accidental presses (you will need a pointed object to use this button).



Figure 100: Reset Button (back of unit)

The actions that are performed when the reset button is pressed are defined in the graphical user interface. Refer to [Security Settings, Encryption & Share](#) for more information.

Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, please refer to [Audit Log](#).

To reset the unit:

1. Power off the Dominion KX II unit.
2. Use a pointed object to press and hold the reset button.
3. **While continuing to hold the reset button**, power the Dominion KX II unit back on.
4. Continue holding the reset button for 5-10 seconds. Once the unit has been reset; two short beeps signal completion.

Starting the KX II Local Console

Simultaneous Users

The Dominion KX II Local Console provides an independent access path to the connected target servers. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to Dominion KX II, you can still simultaneously access your servers from the rack via the Local Console.

Security and Authentication

In order to use the Dominion KX II Local Console, you must first authenticate with a valid username and password. Dominion KX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, Dominion KX II allows access only to those servers to which a user has access permissions (refer to [User Management](#) for additional information on specifying server access and security settings).

If your Dominion KX II has been configured for external authentication services (LDAP, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

***Note:** You can also specify no authentication for local console access; this option is recommended only for secure environments.*

To use the KX II Local Console:

1. You need a keyboard, mouse, and video display connected to the local ports at the back of the Dominion KX II unit. Refer to [Physical Connections](#) for more information about the local port connections.
2. Start the Dominion KX II unit; the KX II Local Console interface displays.

KX II Local Console Interface

The KX II Local Console interface is almost identical to the KX II Remote Console interface. Where there are differences, they are noted in the user manual. Refer to [User Interfaces](#), [KX II Console](#), and [KX II Console Menu Tree](#) for additional information.

Available Resolutions

The KX II Local Console provides the following resolutions to support various monitors:

- 800x600
- 1024x768
- 1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

Accessing Target Servers

Server Display

After you login to the KX II Local Console, the Port Access page opens. This page lists all of the Dominion KX II ports, the connected target servers, and their status and availability.

Raritan. Port Access User Management Device Settings Security Maintenance Diagnostics Local Console Port

Home > Port Access Logout

Port Access

Click on the individual port name to see allowable operations.
1 of 4 Remote KVM channels currently in use.

Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	Lpmachine	up	busy
4	Dominion-KX2_Port4	down	idle
5	Dominion-KX2_Port5	down	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	up	idle
9	Dominion-KX2_Port9	down	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
15	Dominion-KX2_Port15	down	idle
16	Dominion-KX2_Port16	down	idle

Copyright © 2007 Raritan Computer Inc.

Time & Session:
March 02, 2007 14:27:49
User: admin
State: active
Your IP: Local Console
Last Login: Mar 02, 2007 14:12

Device Information:
Device Name: DominionKX
IP Address: 192.168.59.97
Firmware: 2.0.0.2.5282
PowerIn1: on
PowerIn2: off

Port States:
2 Ports up
13 Ports down
14 Ports idle
1 Ports busy

Connected Users:
admin (Local Console)
active
admin (192.168.59.93)
RC active

Figure 101: Local Console Port Access

The target servers are initially sorted by Port Number; you can change the display to sort on any of the columns.

- **Port Number.** Numbered from 1 to the total number of ports available for the Dominion KX II unit. Please note that ports connected to power strips will *not* be among those listed, resulting in gaps in the Port Number sequence.
- **Port Name.** The name of the Dominion KX II port; initially set to Dominion-KX2-Port#, but you can change the name to something more descriptive. When you click on the Port Name link, an Action Menu is opened. Refer to the [Port Action Menu](#) for more information about the menu options available.
- **Status.** The **Status** is either *up* or *down*.
- **Availability.** Valid Values per include *Idle*, *Connected*, *Busy*, or *Unavailable*.

To change the sort order:

Click the column heading you want to sort on. The list of target servers is sorted by that column.

Hotkeys

Because the Dominion KX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hotkey is utilized so you can switch between these interfaces.

The Local Port hotkey allows you to rapidly access the KX II Local Console user interface when a target server is currently being viewed. The default is to press the **Scroll Lock** key twice in rapid succession, but you can designate any key combination (available in the Local Port Settings page) as the hotkey. Refer to [Local Port Settings](#) for more information.

Accessing a Target Server

To access a target server:

1. Click the **Port Name** of the target you want to access. The **Port Action Menu** is displayed.
2. Select **Connect** from the [Port Action Menu](#). The video display switches to the target server interface.

Returning to the KX II Local Console Interface

Important: The KX II Local Console default hotkey is to press the **Scroll Lock** key twice rapidly. This key combination can be changed in the [Local Port Settings](#) page.

To return to the KX II Local Console from the target server:

Press the hotkey (default is **Scroll Lock**) twice rapidly. The video display switches from the target server interface to the Dominion KX II Local Console interface.

Local Port Administration

The Dominion KX II can be managed by either the KX II Local Console or the KX II Remote Console. Please note that the KX II Local Console also provides access to these administrative functions:

- Local Port Settings
- Factory Reset

Note: Only users with administrative privileges can access these functions.

Local Port Settings (KX II Local Console Only)

From the Local Port Settings page, you can customize many settings for the KX II Local Console including keyboard, local port hotkey, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: This feature is available only on the Dominion KX II Local Console.

To configure the local port settings:

1. Select **Device Settings > Local Port Settings**. The Local Port Settings page opens:

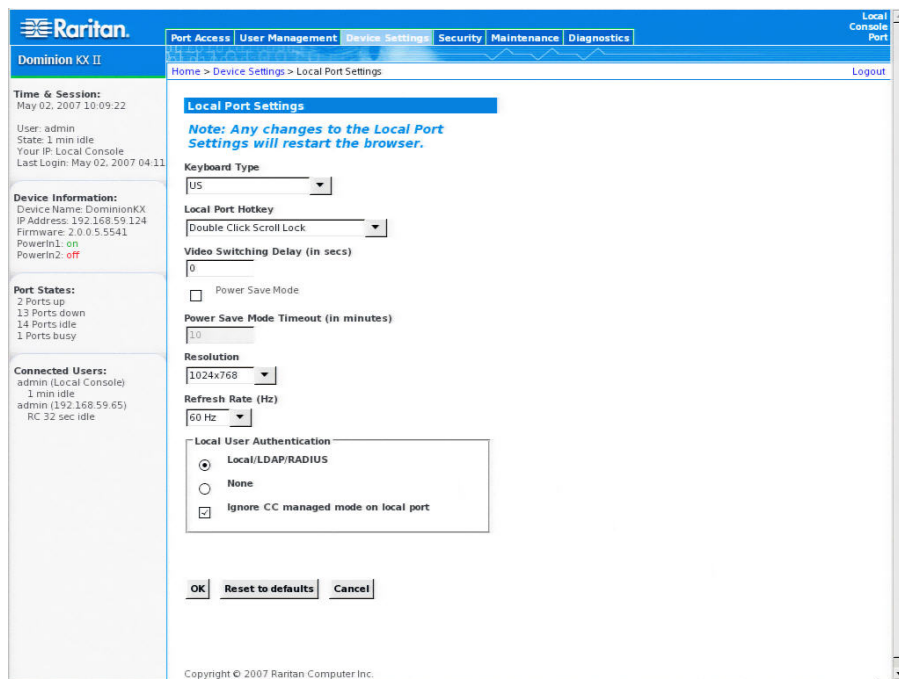


Figure 102: Local Port Settings

2. Select the appropriate **Keyboard Type** from among the options in the drop-down list:

- US
- US/International
- UK
- French
- German
- JIS (Japanese Industry Standard)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)

3. Select the **Local Port Hotkey**. The Local Port Hotkey is used to return to the KX II Local Console interface when a target server interface is being viewed. The default is **Double Click Scroll Lock**, but you can select any key combination from the drop-down list:

HOTKEY:	TAKE THIS ACTION:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

4. Set the **Video Switching Delay** from 0 – 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).
5. If you would like to use the power save feature:
 - a. Check the **Power Save Mode** checkbox.
 - b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.
6. Select the **Resolution** for the KX II Local Console from the drop-down list:
 - 800x600
 - 1024x768
 - 1280x1024
7. Select the **Refresh Rate** from the drop-down list:
 - 60 Hz
 - 75 Hz
8. Select the type of **Local User Authentication**:
 - **Local/LDAP/RADIUS**. This is the recommended option; for more information about authentication, refer to [Remote Authentication](#) and [Authentication vs. Authorization](#).
 - **None**. There is no authentication for local console access. This option is recommended for *secure environments only*.
9. Check the **Ignore CC managed mode on local port** checkbox if you would like local user access to the Dominion KX II even when the device is under CC-SG management.

Note: If you clear this checkbox but then want local port access, you will have to remove the device from under CC-SG management (from within CC-SG) and then you will be able to check this checkbox.

10. Click **OK**.

To close the page without saving any changes:

Click **Cancel**.

To reset back to defaults:

Click **Reset to Defaults**.

Factory Reset (KX II Local Console Only)

***Note:** This feature is available only on the Dominion KX II Local Console.*

The Dominion KX II offers several types of reset modes from the Local Console user interface.

***Note:** It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, please refer to [Audit Log](#).*

To perform a factory reset:

1. Select **Maintenance > Factory Reset**. The Factory Reset page opens:

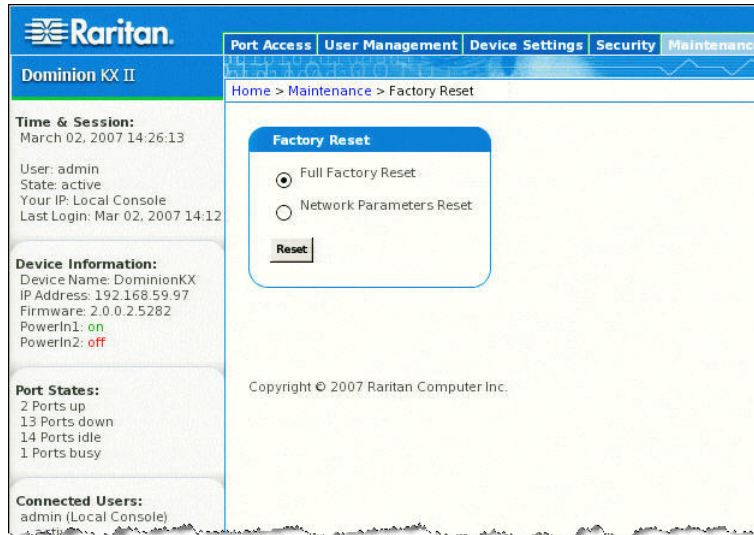


Figure 103: Factory Reset (Local Console Only)

2. Select the appropriate reset option.
 - **Full Factory Reset:** Removes the entire configuration and resets the unit completely to the factory defaults. Please note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
 - **Network Parameter Reset:** Resets the network parameters (from **Device Settings > Network Settings**) of the unit back to the default values:

IP auto configuration
IP Address
Subnet Mask
Gateway IP address
Primary DNS server IP address
Secondary DNS server IP address
Discovery Port
Bandwidth Limit
LAN Interface Speed & Duplex
Enable Automatic Failover
Ping Interval (seconds)
Timeout (Seconds)

You will be prompted to confirm this action because all network settings will be permanently lost.

3. Click **Reset** to continue. You will be prompted to confirm the factory reset.
4. Click the **Really Reset** button to proceed. Upon completion, the Dominion KX II unit is automatically restarted.

Chapter 14: CC Unmanage

Overview

When a Dominion KX II device is under CommandCenter Secure Gateway control and you attempt to access the device directly using the Dominion KX II Remote Console, the following message is displayed (after entry of a valid username and password):



Figure 104: Device Managed by CC-SG Message

Removing Dominion KX II from CC-SG Management

Unless the Dominion KX II is released from CC-SG control, you cannot access the device directly. If, however, the KX II does not receive heartbeat messages from CommandCenter (e.g., CommandCenter is not on the network), you can release the KX II from CC-SG control in order to access the device. This is accomplished by using the CC Unmanage feature.

Note: Maintenance permission is required to use this feature.

When no heartbeat messages are received, the following message is displayed when attempting to access the device directly:

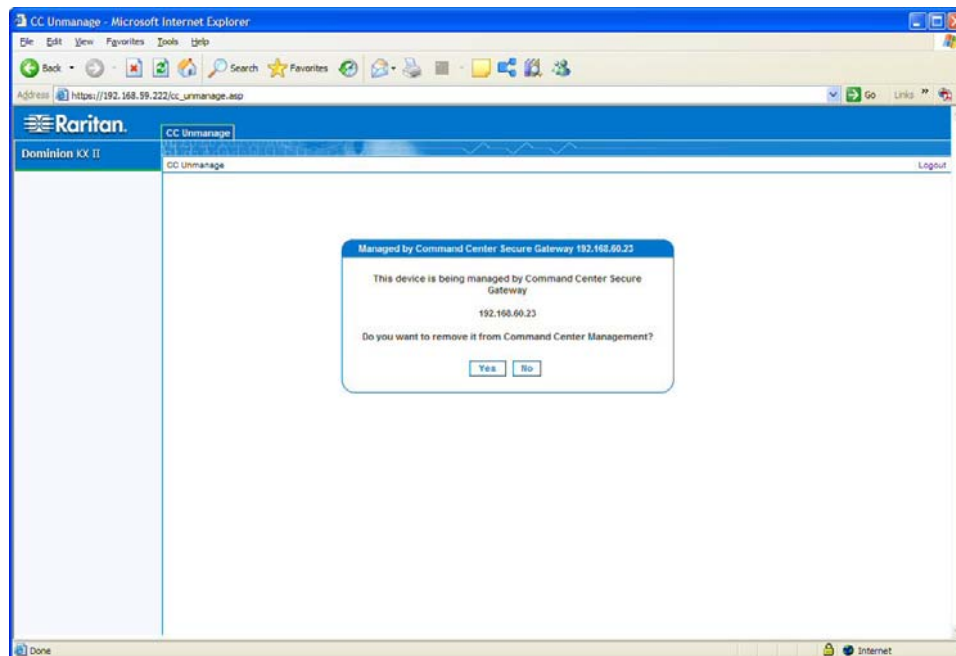


Figure 105: Remove from CC-SG Management

To remove the device from CC-SG management (to use CC Unmanage):

1. Click the **Yes** button. You are prompted to confirm the action:

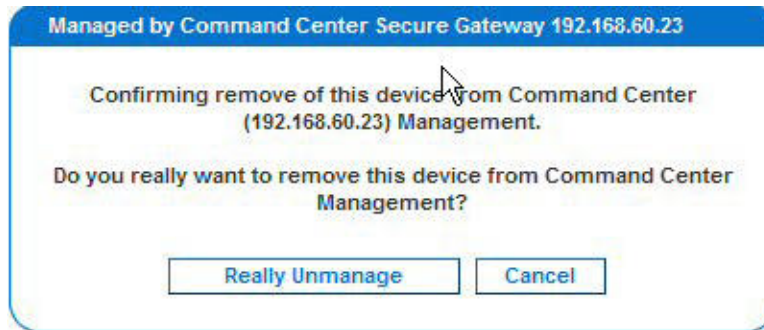


Figure 106: Confirm CC Unmanage

2. Click the **Really Unmanage** button. A message is displayed confirming that the device is no longer under CC management:

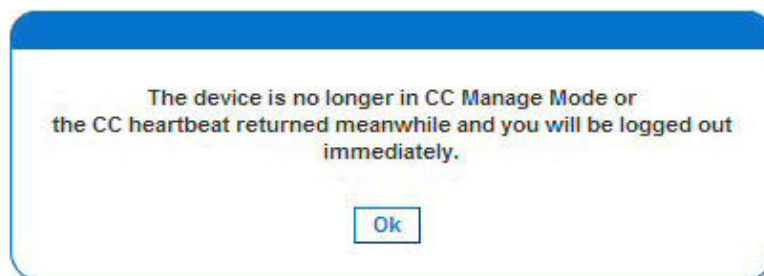


Figure 107: Device Removed from CC Management

3. Click **OK**. The Dominion KX II login page opens.

Appendix A: Specifications

Environmental Requirements

OPERATING	
Temperature	0°C - 40°C (32°F - 104°F)
Humidity	20% - 85% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
NON-OPERATING	
Temperature	0°C - 50°C (32°F - 122°F)
Humidity	10% - 90% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

Physical Specifications

PART NUMBER	DKX2-116	DKX2-132	DKX2-216	DKX2-232	DKX2-416	DKX2-432
Line Item Description	16-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	16-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	16-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power
Weight	8.65 lbs; 3.9kg	9.0 lbs; 4.1kg	8.65 lbs; 3.9 kg	9.0 lbs; 4.1 kg	9.04 lbs; 4.1 kg	9.48 lbs; 4.3 kg
Product Dimensions (WxDxH)	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm
Shipping Weight	14.85 lbs; 6.7 kg	14.9 lbs; 6.8 kg	14.49 lbs; 6.6 kg	14.9 lbs; 6.8 kg	14.94 lbs; 6.8 kg	15.38 lbs; 7.0 kg
Shipping Dimensions (WxDxH)	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm
UPC Code	785813624055	785813624079	785813624086	785813625021	785813625359	785813625380
Power	Dual Power 100/240 V 50/60 Hz 0.6A 25.4 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 26 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 26.3 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 27 Watts	Dual Power 100/240 V 50/60 Hz 1A 62 Watts	Dual Power 100/240 V 50/60 Hz 1A 64 Watts

Electrical Specifications

PARAMETER		VALUE
Input		
	Nominal Frequencies	50/60 Hz
	Nominal Voltage Range	100/240 VAC
	Maximum Current AC RMS	0.6A max.
	AC Operating Range	100 to 240 VAC (+-10%), 47 to 63 Hz
Output		
	+5 VDC, +12VDC	N/A
	-5 VDC, -12VDC	N/A
	Maximum DC Power Output	N/A
	Maximum AC Power Consumption	N/A
	Maximum Heat Dissipation	N/A
	Volt-Ampere Rating	N/A

Computer Interface Modules (CIMs)

PART NUMBER	D2CIM-VUSB	DCIM-PS2	DCIM-USB	DCIM-SUSB
Line Item Description	Dominion KX II Computer Interface Module [USB Port with Virtual Media]	Dominion KX I & II Computer Interface Module [PS/2 Port]	Dominion KX I & II Computer Interface Module [USB Port]	Dominion KX I & II Computer Interface Module [USB Port for Sun]
Product Weight	0.2 lbs	0.2 lbs	0.2 lbs	0.2 lbs
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"
Shipping Weight	0.2 lbs	0.2 lbs	0.2 lbs	0.2 lbs
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"
UPC Code	785813332004	785813338532	785813338518	785813338556

PART NUMBER	DCIM-SUN	D2CIM-PWR	D2CIM-VUSB-32PAC	D2CIM-VUSB - 64PAC
Line Item Description	Dominion KX I & II Computer Interface Module [Sun Port, HD15 Video]	Dominion KX II Computer Interface Module for Remote Power strips	Bulk pack of 32 D2CIM-VUSB	Bulk pack of 64 D2CIM-VUSB
Product Weight	0.2 lbs	0.2 lbs	6.4 lb	12.8 lb
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	(1.3" x 3.0" x 0.6")*32	(1.3" x 3.0" x 0.6")*64
Shipping Weight	0.2 lbs	0.2 lbs	8.01 lb	18.13 lb
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	21.65"x12.20"x4.33"	22.64"x9.45"x12.99"
UPC Code	785813338549	785813332011	785813332028	785813332035

Remote Connection

Network: 10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
 Protocols: TCP/IP, UDP, SNMP, HTTP, HTTPS, RADIUS, LDAP

KVM Properties

Keyboard: PS/2 or USB
 Mouse: PS/2 or USB
 Video: VGA

TCP and UDP Ports Used

- **HTTP, Port 80** – All requests received by Dominion KX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. Dominion KX II responds to Port 80 for user convenience, relieving users from having to explicitly type “https://” in the URL field to access Dominion KX II, but while still preserving complete security.
- **HTTPS, Port 443** – This port is used for a single purpose only: to send the Dominion KX II Web-accessible clients (KX II Console, MPC) to the user. No other communication occurs on this port. If you do not wish to use the Dominion KX II Web-access capabilities and instead prefer to use the installed client software provided on the CD-ROM, you can prevent access to Port 443 via your firewall and Dominion KX II can still function.
- **Dominion KX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000** – With the exception of the ports above, all communication to Dominion KX II occurs over a single, configurable TCP Port. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, refer to [Network Settings](#).
- **SNTP (Time Server) on Configurable UDP Port 123 (optional)** – Dominion KX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation.
- **LDAP on Configurable Ports 389 and 636 (optional)** – If Dominion KX II is configured to remotely authenticate user logins via the LDAP protocol, ports 389 and 636 will be used, but the system can also be configured to use any port of your designation.
- **RADIUS on Configurable Port 1812 (optional)** – If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 or 1813 will be used, but the system can also be configured to use any port of your designation.
- **RADIUS Accounting on Configurable Port 1813** – If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.
- **SYSLOG on Configurable UDP Port 514** – If Dominion KX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
- **SNMP Default UDP Ports (optional)** – Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps.
- **UDP Port 21** – Port 21 is used for the Dominion KX II command line interface (when you are working with Raritan Technical Support).

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat 5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations. The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

VIDEO RESOLUTION	REFRESH RATE	MAXIMUM DISTANCE
1600x1200	60	50 ft (15 m)
1280x1024	60	100 ft (30 m)
1024x768	60	150 ft (45 m)

The use of Paragon CIMs will not increase the distance between the Dominion KX II and the target server.

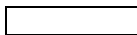
Due to the multiplicity of server manufacturers and types, OS versions, video drivers, etc. and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

Refer to the [Supported Video Resolutions](#) for the video resolutions supported by Dominion KX II.

Network Speed Settings

		DOMINION KX II NETWORK SPEED SETTING					
		AUTO	1000/FULL	100/FULL	100/HALF	10/FULL	10/HALF
NETWORK SWITCH PORT SETTING	AUTO	highest available speed	1000/Full	KX: 100/Full Switch: 100/Half	100/Half	KX: 10/Full Switch: 10/Half	10/Half
	1000/FULL	1000/Full	1000/Full	no communication	no communication	no communication	no communication
	100/FULL	KX: 100/Half Switch: 100/Full	KX: 100/Half Switch: 100/Full	100/Full	KX: 100/Half Switch: 100/Full	no communication	no communication
	100/HALF	100/Half	100/Half	KX: 100/Full Switch: 100/Half	100/Half	no communication	no communication
	10/FULL	KX: 10/Half Switch: 10/Full	no communication	no communication	no communication	10/Full	KX: 10/Half Switch: 10/Full
	10/HALF	10/Half	no communication	no communication	no communication	KX: 10/Full Switch: 10/Half	10/Half

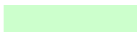
Legend:



Does not function, as expected



Supported



Functions; not recommended



NOT supported by Ethernet specification; product will communicate, but collisions will occur



Per Ethernet specification, these should be “no communication”, however, note that the Dominion KX II behavior deviates from expected behavior

Note: For reliable network communication, configure the Dominion KX II and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Appendix B: Updating the LDAP Schema

Note: The procedures in this chapter should be attempted only by experienced users.

Returning User Group Information

Use the information in this chapter to return User Group information (and assist with authorization) once authentication is successful.

From LDAP

When an LDAP authentication is successful, Dominion KX II determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

```
rciusergroup          attribute type: string
```

This may require a schema extension on your LDAP server. Consult your authentication server administrator to enable this attribute.

In addition, the standard LDAP `memberOf` is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory administrator.

Returning user group information from Microsoft's Active Directory for Windows 2000 Server requires updating the LDAP schema. Refer to your Microsoft documentation for more detail.

1. Install the schema plug-in for Active Directory – refer to Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select **Active Directory Schema**.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

1. Right-click the **Active Directory Schema** root node in the left pane of the window, and then click **Operations Master**.
2. Check the checkbox before **The Schema may be modified on this Domain Controller**.
3. Click **OK**.

Creating a New Attribute

To create new attributes for the **rciusergroup** class:

1. Click the + symbol before **Active Directory Schema** in the left pane of the window.
2. Right-click **Attributes** in the left pane.
3. Click **New**, and then select **Attribute**. When the warning message appears, click **Continue** and the **Create New Attribute** window appears.

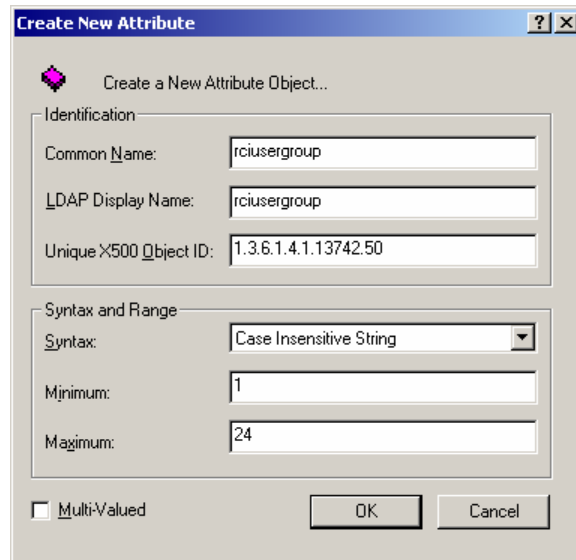


Figure 108: Create New Attribute

4. Type **rciusergroup** in the **Common Name** field.
5. Type **rciusergroup** in the **LDAP Display Name** field.
6. Type **1.3.6.1.4.1.13742.50** in the **Unique x5000 Object ID** field.
7. Click on the **Syntax** drop-down arrow and select **Case Insensitive String** from the list.
8. Type **1** in the **Minimum** field.
9. Type **24** in the **Maximum** field.
10. Click **OK** to create the new attribute.

Adding Attributes to the Class

1. Click **Classes** in the left pane of the window.
2. Scroll to the **user** class in the right pane, and right-click on it.
3. Select **Properties** from the menu. The **user Properties** window appears.
4. Click on the **Attributes** tab.
5. Click **Add**.
6. Select **rciusergroup** from the **Select Schema Object** list.

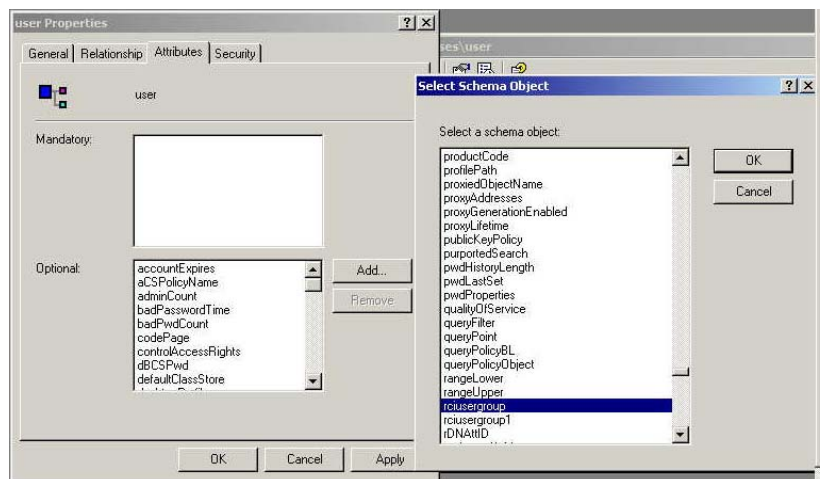


Figure 109: Adding the Attributes to the Class

7. Click **OK**.
8. Click **OK**.

Updating the Schema Cache

1. Right-click **Active Directory Schema** in the left pane of the window and select **Reload the Schema** from the shortcut menu.
2. Minimize the Active Directory Schema MMC console.

Editing RCI User Group Attributes for User Members

To run Active Directory script on Windows 2003 server, please use the script provided by Microsoft. These scripts are loaded onto your system with a Microsoft Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service. For additional information, visit Microsoft's Web site:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebca3324-5427-471a-bc19-9a1decd3d40.mspx>.

To edit the individual user attributes within the group **rciusergroup**:

1. On the Windows **Start** menu, click **Run**.
2. Type **regsvr adsiedit.msc**. The ADSI Edit window appears.

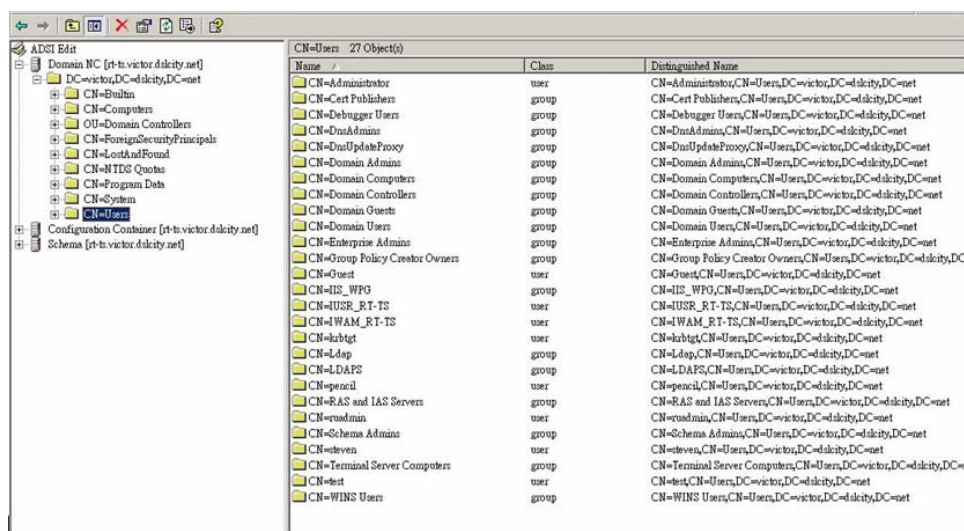


Figure 110: ADSI Edit

3. In the left pane of the window, select the **CN=User** folder.
4. Locate the user name whose properties you want to adjust in the right pane. Right-click on the user name and select **Properties**.
5. Click on the **Attributes** tab.

6. Click on the **Select a property to view** drop-down arrow and select **rciusergroup** from the list.

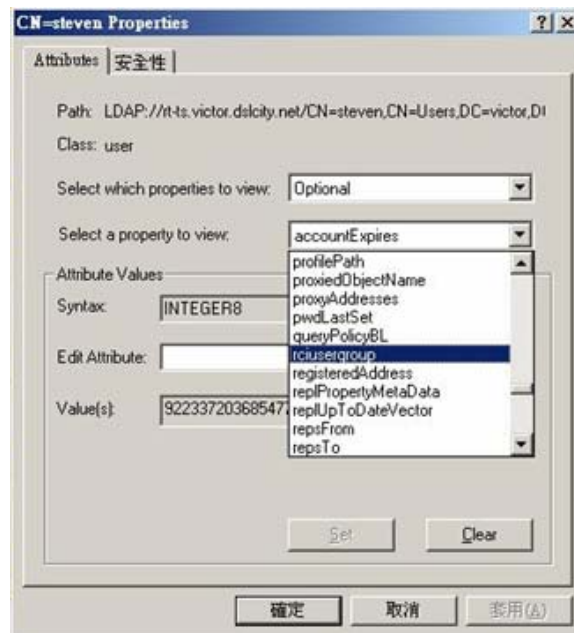


Figure 111: User Properties

7. In the **Attribute Values** panel of the window, type the user name you would like returned to RRC in the **Edit Attribute** field.

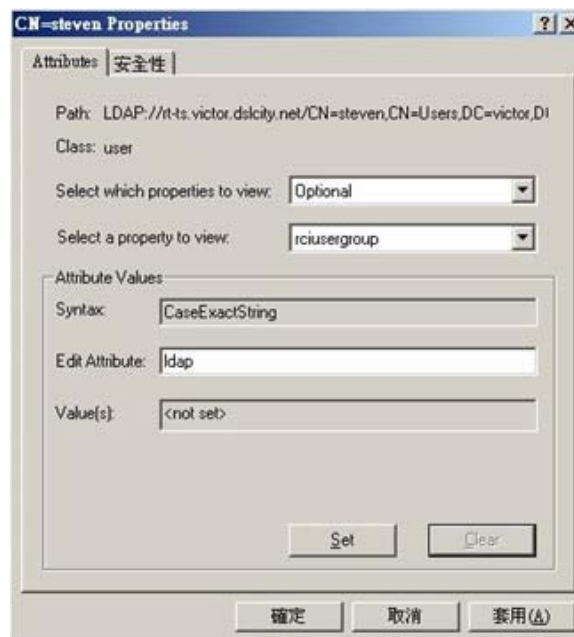


Figure 112: Edit Attribute (adding user to KX II group)

8. Click **Set**.
9. Click **OK**.

Appendix C: Informational Notes

Overview

This chapter includes important notes on Dominion KX II usage. Future updates will be documented and available online through the Help – User Guide link in the KX II Remote Console interface.

Non-US Keyboards

French Keyboard

Caret Symbol (Linux Clients only)

The Virtual KVM Client and the Multi-Platform Client (MPC) do not process the key combination of **Alt Gr + 9** as the caret symbol (^) when using French keyboards with Linux clients.

To obtain the caret symbol:

From a French keyboard, press the ^ key (to the right of the **P** key), then *immediately* press the **spacebar**.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9
3. Release 9
4. Release Right Alt

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the **P** key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP Clients only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of **Alt Gr + 7** results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

NUMERIC KEYPAD SYMBOL	DISPLAYS AS
/	;
.	;

Tilde Symbol

From the Virtual KVM Client and the Multi-Platform Client, the key combination of **Alt Gr + 2** does not produce the tilde (~) symbol when using a French keyboard.

To obtain the tilde symbol:

Create a macro consisting of the following commands:

1. Press Right Alt
2. Press 2
3. Release 2
4. Release Right Alt

Java Runtime Environment (JRE)

Because of a limitation in the Java Runtime Environment (JRE), Fedora, Linux, and Solaris clients receive an invalid response from **Alt Gr** on UK English and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the **Alt Gr** key combination for Java 1.4.2 or 1.5. Java 1.6 appears to improve on this, although the *keyPressed* and *keyReleased* events for **Alt Gr** still identify it as an “unknown key code”.

Also, a key pressed in combination with **Alt Gr** (such as on the UK keyboard **Alt Gr-4**), which is the Euro symbol), will only generate a *keyTyped* followed by a *keyReleased* event for that value, without a *keyPressed* event. Java 1.6 improves upon this by filling in the *keyPressed* event as well.

Keyboard Language Preference (Fedora Linux Clients)

There are several methods that can be used to set the keyboard language preference on Fedora Linux clients. The following method *must* be used in order for the keys to be mapped correctly from the Virtual KVM Client and the Multi-Platform Client (MPC).

To set the keyboard language:

1. From the toolbar, select **System > Preferences > Keyboard**.
2. Open the **Layouts** tab.
3. Add or select the appropriate language.
4. Click **Close**.

***Note:** Other methods will not necessarily yield correct results.*

Macintosh Keyboard

When a Macintosh is used as the client, the following keys on the Mac keyboard are not captured by the Java Runtime Environment (JRE):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora, the target and local mouse pointers may lose synchronization after some time.

To re-synchronize the mouse cursors:

Use the Synchronize Mouse option from the Virtual KVM Client.

The following table summarizes the Dominion KX II mouse modes, and whether or not these modes remain synchronized when accessing target servers running Fedora:

MOUSE MODE	FEDORA CORE 5	FEDORA CORE 6
Absolute Mouse Synchronization™	No	No
Intelligent Mouse Mode	No	Yes
Standard Mouse Mode	Yes	No

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log into a Dominion KX II device or to access target servers (Windows, SUSE, etc.). In addition, the **Ctrl+Alt+M** key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora Core 6 and Firefox 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey™ (formerly Mozilla) browser to work with the Java plugin.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). Dominion KX II, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

To configure the SUSE video display:

1. The generated configuration file `/etc/X11/xorg.conf` includes a "Monitor" section with an option named `UseModes`. For example:
`UseModes "Modes[0]"`
2. Either comment out this line (using `#`) or delete it completely.
3. Restart the X server.

With this change, the internal video mode timing from the X server will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the Dominion KX II.

CIMs

Windows 3-Button Mouse on Linux Targets

When using a 3-button mouse on a Windows client connecting to a Linux target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Virtual Media

Dell OptiPlex and Dimension Computers

From certain Dell OptiPlex and Dimension computers, it may not be possible to boot a target server from a redirected drive/ISO image, or to access the target server BIOS when a virtual media session is active (unless the **Use Full Speed for Virtual Media CIM** option is enabled from the Port page).

Virtual Media not Refreshed after Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

To shorten the boot time:

1. Close the Virtual KVM Client to completely release the virtual media drives.
2. Restart the target.

CC-SG

Virtual KVM Client Version not Known from CC-SG Proxy Mode

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is *unknown*. In the About Raritan Virtual KVM Client dialog, the version is displayed as “Version Unknown”.

Proxy Mode and MPC

If you are using Dominion KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC).

Appendix D: FAQs

General Questions

QUESTION	ANSWER
What is Dominion KX II?	<p>Dominion KX II is a second generation digital KVM (Keyboard, Video Mouse) switch that enables IT administrators to access and control 16, 32, or 64* servers over the network with BIOS-level functionality. Dominion KX II is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.</p> <p>At the rack, Dominion KX II provides the same functionality, convenience, space savings, and cost savings as traditional analog KVM switches. However, Dominion KX II also integrates the industry's highest-performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation.</p>
How does Dominion KX II differ from remote control software?	<p>When using Dominion KX II remotely, at first glance, the interface may seem similar to remote control software such as pcAnywhere™, Windows® Terminal Services / Remote Desktop, VNC, etc. However, because Dominion KX II is not a software but a hardware solution, it's much more powerful:</p> <ul style="list-style-type: none"> • OS- and hardware-independent – Dominion KX II can be used to manage servers running many popular operating systems, including Intel®, Sun®, PowerPC running Windows, Linux®, Solaris™, etc. • State-independent / Agentless – Dominion KX II does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server. • Out-of-Band – Even if the managed server's own network connection is unavailable, it can still be managed through Dominion KX II. • BIOS-level access – Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, Dominion KX II still works flawlessly to enable these configurations to be made.
How do the new features of the Dominion KX II compare to the KX I?	Dominion KX II has many new and exciting features, including virtual media, dual power, dual gigabit Ethernet, common Web-based user interfaces, next generation local port, etc.
How do I migrate from the Dominion KX I to Dominion KX II?	In general, KX I customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new KX II models. Raritan's centralized management appliance, CommandCenter® Secure Gateway, and the Multi-Platform Client (MPC) both support KX I and KX II switches seamlessly.
Will my existing KX I CIMs work with the Dominion KX II switch?	Yes, existing KX I CIMs will work with the Dominion KX II switch. In addition, select Paragon CIMs will work with the KX II. This provides an easy migration to KX II from Paragon I customers who wish to switch to KVM-over-IP.

QUESTION	ANSWER
Can the Dominion KX II be rack mounted?	Yes. The Dominion KX II ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.
How large is the Dominion KX II?	Dominion KX II is only 1U high (except KX2-464, which is 2U), fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep.

Remote Access

QUESTION	ANSWER															
How many users can remotely access servers on each Dominion KX II?	Dominion KX II models offer remote connections for up to eight users per channel for simultaneous access and control of a unique target server. For one-channel devices like the DKX2-116, up to eight remote users can access and control a single target server. For two-channel devices, like the DKX2-216, up to eight users can access and control the server on channel one and up to another eight users on channel two. For four-channel devices, up to eight users per channel, for a total of 32 (8 x 4) users, can access and control four servers in a similar fashion.															
Can two people look at the same server at the same time?	Yes, actually up to eight people can access and control any single server at the same time.															
Can two people access the same server, one remotely and one from the local port?	Yes, the local port is completely independent of the remote “ports.” The local port can access the same server using the PC-Share feature.															
In order to access Dominion KX II from a client, what hardware, software or network configuration is required?	<p>Because Dominion KX II is completely Web-accessible, it doesn’t require installation of proprietary software on clients used for access. (An optional installed client is available on Raritan.com for the purposes of accessing Dominion KX II via modem).</p> <p>Dominion KX II can be accessed through major Web browsers including: Internet Explorer, Mozilla™ and Firefox. Dominion KX II can now be accessed on Windows, Linux, Sun Solaris and Macintosh® desktops, via Raritan’s Java-based Multi-Platform Client (MPC) and the new Virtual KVM Client™.</p> <p>Dominion KX II administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.</p>															
What is the file size of the applet that is used to access Dominion KX II? How long does it take to retrieve?	<p>The Virtual KVM Client applet used to access Dominion KX II is approximately 500KB in size. The following chart describes the time required to retrieve Dominion KX II’s applet at different network speeds:</p> <table><tr><td>100Mbps</td><td>Theoretical 100Mbit network speed</td><td>0.05 seconds</td></tr><tr><td>60Mbps</td><td>Likely practical 100Mbit network speed</td><td>0.08 seconds</td></tr><tr><td>10Mbps</td><td>Theoretical 10Mbit network speed</td><td>.4 seconds</td></tr><tr><td>6Mbps</td><td>Likely practical 10Mbit network speed</td><td>.8 seconds</td></tr><tr><td>512Kbps</td><td>Cable modem download speed (typical)</td><td>8 seconds</td></tr></table>	100Mbps	Theoretical 100Mbit network speed	0.05 seconds	60Mbps	Likely practical 100Mbit network speed	0.08 seconds	10Mbps	Theoretical 10Mbit network speed	.4 seconds	6Mbps	Likely practical 10Mbit network speed	.8 seconds	512Kbps	Cable modem download speed (typical)	8 seconds
100Mbps	Theoretical 100Mbit network speed	0.05 seconds														
60Mbps	Likely practical 100Mbit network speed	0.08 seconds														
10Mbps	Theoretical 10Mbit network speed	.4 seconds														
6Mbps	Likely practical 10Mbit network speed	.8 seconds														
512Kbps	Cable modem download speed (typical)	8 seconds														
How do I access servers connected to Dominion KX II if the network ever becomes unavailable?	Dominion KX II offers a dedicated modem port for attaching an external modem. With an externally-connected modem, servers can still be remotely accessed in the event of a network emergency. Furthermore, Dominion KX II’s local ports always allow access to servers from the rack, regardless of the network condition.															

QUESTION	ANSWER
Do you have a non-Windows client?	Yes. Both the Virtual KVM Client and the Multi-Platform Client (MPC), allow non-Windows users to connect to target servers through the Dominion KX I and KX II switches. MPC can be run via Web browsers and standalone. Please refer to the Virtual KVM Client and the <i>MPC/RRC User Guide</i> for more information.
My modem connection dropped and I got the error message “There was an unexpected communications error – connection terminated.” What should I do?	This might have happened based on the frequency with which the user tried to connect via modem. Reboot the KX unit and modem, and for future connections, wait at least two (2) minutes between attempts.
Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do?	<p>This usually occurs in situations when the Alt key is held and <u>not</u> released. For instance, continuing to press the Alt key while pressing the space bar might cause the focus to change from the target server to the client PC.</p> <p>The local operating system then interprets this key combination and consequently triggers the action for this key combination in the active window (the client PC).</p>

Universal Virtual Media

QUESTION	ANSWER
What Dominion KX II models support virtual media?	All Dominion KX II models support virtual media. It is available standalone and through CommandCenter Secure Gateway, a centralized management appliance.
What types of virtual media does the Dominion KX II support?	Dominion KX II supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives, and remote drives.
What is required for virtual media?	The new D2CIM-VUSB CIM is required for virtual media. It supports virtual media sessions to target servers supporting the USB 2.0 interface. Available in economical 32 and 64 quantity CIM packages, this new CIM supports Absolute Mouse Synchronization as well as remote firmware update.
Is virtual media secure?	Yes. Virtual media sessions are secured using 128-bit AES or RC4 encryption.

Ethernet and IP Networking

QUESTION	ANSWER												
Does the Dominion KX II offer dual gigabit Ethernet ports to provide redundant fail-over, or load balancing?	Yes. Dominion KX II features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, Dominion KX II will failover to the secondary network port with the same IP address – ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.												
How much bandwidth does Dominion KX II require?	<p>Dominion KX II offers next generation KVM-over-IP technology – the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.</p> <p>Raritan pioneered the KVM-over-IP functionality that allows users to tailor their video parameters to conserve network bandwidth. For instance, when connecting to Dominion KX II through a dial-up modem connection, video transmissions can be scaled to grayscale – allowing users to be fully productive while ensuring high performance.</p> <p>With that in mind, the following data refers to Dominion KX II at its default video settings – again, these settings can be tailored to a specific environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections.</p> <p>As a general rule, a conservative estimate for bandwidth utilization (at Dominion KX II's default settings) is approximately 0.5Mbit/second per active KVM user (connected to and using a server), with very occasional spikes up to 2Mbit/second. This is a very conservative estimate because bandwidth utilization will typically be even lower.</p> <p>Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The table below summarizes some use cases and the required bandwidth utilization at Dominion KX II's default settings on a 10Mbit/s network:</p> <table border="1"> <tr> <td>Idle Windows Desktop</td><td>0 Mbps</td></tr> <tr> <td>Move Cursor Around Desktop</td><td>0.18Mbps</td></tr> <tr> <td>Move Static 400x600 Window/Dialog Box</td><td>0.35Mbps</td></tr> <tr> <td>Navigate Start Menu</td><td>0.49Mbps</td></tr> <tr> <td>Scroll an Entire Page of Text</td><td>1.23Mbps</td></tr> <tr> <td>Run 3D Maze Screensaver</td><td>1.55Mbps</td></tr> </table>	Idle Windows Desktop	0 Mbps	Move Cursor Around Desktop	0.18Mbps	Move Static 400x600 Window/Dialog Box	0.35Mbps	Navigate Start Menu	0.49Mbps	Scroll an Entire Page of Text	1.23Mbps	Run 3D Maze Screensaver	1.55Mbps
Idle Windows Desktop	0 Mbps												
Move Cursor Around Desktop	0.18Mbps												
Move Static 400x600 Window/Dialog Box	0.35Mbps												
Navigate Start Menu	0.49Mbps												
Scroll an Entire Page of Text	1.23Mbps												
Run 3D Maze Screensaver	1.55Mbps												
What is the slowest connection (lowest bandwidth) over which Dominion KX II can operate?	33Kbps or above is recommended for acceptable KX performance over a modem connection.												
What is the speed of Dominion KX II's Ethernet interfaces?	Dominion KX II supports Gigabit as well as 10/100 Ethernet. KX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).												

QUESTION	ANSWER
Can I access Dominion KX II over a wireless connection?	Yes. Dominion KX II not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to a Dominion KX II, servers can be configured and managed at BIOS-level wirelessly.
Can Dominion KX II be used over the WAN (Internet), or just over the corporate LAN?	Whether via a fast corporate LAN, the less predictable WAN (Internet), cable modem or dial-up modem, Dominion KX II's KVM-over-IP technology can accommodate the connection.
Can I use Dominion KX II with a VPN?	Yes. Dominion KX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.
How many TCP ports must be open on my firewall in order to enable network access to Dominion KX II? Are these ports configurable?	Only one. Dominion KX II protects network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security. Note that, of course, to use Dominion KX II's optional Web browser capability, the standard HTTPS port 443 must also be open.
Does Dominion KX II require an external authentication server to operate?	No. Dominion KX II is a completely self-sufficient appliance. After assigning an IP address to a Dominion KX II, it is ready to use – with Web browser and authentication capabilities completely built-in. If an external authentication server (such as LDAP, Active Directory®, RADIUS, etc.) is used, Dominion KX II allows this as well, and will even failover to its own internal authentication should the external authentication server become unavailable. In this way, Dominion KX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.
Can Dominion KX II be used with CITRIX?	Dominion KX II may work with remote access products like CITRIX if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.
Can the Dominion KX II use DHCP?	DHCP addressing can be used, however, Raritan recommends fixed addressing since the Dominion KX II is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.

QUESTION	ANSWER
I'm having problems connecting to the Dominion KX II over my IP network. What could be the problem?	<p data-bbox="573 149 1321 212">The Dominion KX II relies on your LAN/WAN network. Some possible problems include:</p> <ul data-bbox="623 233 1409 751" style="list-style-type: none"><li data-bbox="623 233 1409 359">• Ethernet auto negotiation. On some networks, 10/100 auto negotiation does not work properly and the KX II unit must be set to 100MB/full duplex or the appropriate choice for its network.<li data-bbox="623 380 1409 485">• Duplicate IP Address. If the IP Address of the KX II is the same as another device, network connectivity may be inconsistent.<li data-bbox="623 506 1409 611">• Port 5000 conflicts. If another device is using port 5000, the KX II default port must be changed (or the other device must be changed).<li data-bbox="623 632 1409 751">• When changing the IP Address of a KX II, or swapping in a new KX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.

Servers

QUESTION	ANSWER
Does Dominion KX II depend on a Windows server to operate?	<p>Absolutely not. Because users depend on the KVM infrastructure to always be available in any scenario whatsoever (as they will likely need to use the KVM infrastructure to fix problems), Dominion KX II is designed to be completely independent from any external server.</p> <p>For example, should the data center come under attack from a malicious Windows worm or virus, administrators will need to use the KVM solution to resolve the situation. Therefore, it is imperative that the KVM solution, in turn, must not rely on these same Windows servers (or any server, for that matter) to be operational in order for the KVM solution to function.</p> <p>To this end, Dominion KX II is completely independent. Even if a user chooses to configure the Dominion KX II to authenticate against an Active Directory server – if that Active Directory server becomes unavailable, Dominion KX II's own authentication will be activated and fully functional.</p>
Do I need to install a Web server such as Microsoft Internet Information Services (IIS) in order to use Dominion KX II's Web browser capability?	No. Dominion KX II is a completely self-sufficient appliance. After assigning an IP address to Dominion KX II, it's ready to use – with Web browser and authentication capabilities completely built-in.
What software do I have to install in order to access Dominion KX II from a particular workstation?	None. Dominion KX II can be accessed completely via a Web browser (although an optional installed client is provided on Raritan's Web site Raritan.com for the purpose of accessing Dominion KX II via modem). A Java-based client is now available for non-Windows users.
What should I do to prepare a server for connection to Dominion KX II?	Simply set the mouse parameters in order to provide users with the best mouse synchronization during remote connections, as well as turning off the power management features that effect screen display. However, if the new D2CIM-VUSB adapter is used (supporting Absolute Mouse Synchronization™), then manually setting the mouse parameters isn't necessary.
What comes in the Dominion KX II box?	The following is included: (a) Dominion KX II unit; (b) Quick Setup Guide; (c) standard 19" rack mount brackets; (d) User manual CD-ROM; (e) Network cable; (f) Crossover cable; (g) Localized AC Line Cord; (h) Warranty certificate and other documentation.

Installation

QUESTION	ANSWER
Besides the unit itself, what do I need to order from Raritan to install Dominion KX II?	Each server that connects to Dominion KX II requires a Dominion or Paragon Computer Interface Module (CIM), an adapter that connects directly to the keyboard, video, and mouse ports of the server.
What kind of Cat5 cabling should be used in my installation?	Dominion KX II can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say “Cat5” cabling for short. In actuality, any brand UTP cable will suffice for Dominion KX II.
What types of servers can be connected to Dominion KX II?	Dominion KX II is completely vendor independent. Any server with standard-compliant keyboard, video, and mouse ports can be connected.
How do I connect servers to Dominion KX II?	Servers that connect to the Dominion KX II require a Dominion or Paragon CIM, which connects directly to the keyboard, video, and mouse ports of the server. Then, connect each CIM to Dominion KX II using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.
How far can my servers be from Dominion KX II?	In general servers can be up to 150 feet (45 m) away from Dominion KX II depending on the type of server. (Please refer to the Raritan Web site or Target Server Connection Distance for more information.) For the new D2CIM-VUSB CIM that supports virtual media and Absolute Mouse Synchronization, a 100 (30 m) foot range is recommended.
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to Dominion KX II from locking up when I switch away from them?	Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan’s KME technology is data center grade, battle-tested, and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.
Are there any agents that must be installed on servers connected to Dominion KX II?	Servers connected to Dominion KX II do not require any software agents to be installed, because Dominion KX II connects directly via hardware to servers’ keyboard, video, and mouse ports.
How many servers can be connected to each Dominion KX II unit?	Dominion KX II models range from 16 or 32 server ports in a 1U chassis to 64 server ports in a 2U chassis. This is the industry’s highest digital KVM switch port density.
What happens if I disconnect a server from Dominion KX II and reconnect it to another Dominion KX II unit, or connect it to a different port on the same Dominion KX II unit?	Dominion KX II will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management appliance.

QUESTION	ANSWER
How do I connect a serially controlled (RS-232) device to Dominion KX II, such as a Cisco router/switch or a headless Sun server?	<p>If there are only a few serially-controlled devices, they may be connected to a Dominion KX II using Raritan's new P2CIM-SER serial converter.</p> <p>However, if there are four or more serially-controlled devices, we recommend the use of Raritan's Dominion SX line of secure console servers. For multiple serial devices, Dominion SX offers more serial functionality at a better price point than Dominion KX II. This SX is easy to use, configure and manage, and can be completely integrated with a Dominion Series deployment. In particular, many UNIX and networking administrators appreciate the ability to directly SSH to a Dominion SX unit.</p>

Local Port

QUESTION	ANSWER
Can I access my servers directly from the rack?	Yes. At the rack, Dominion KX II functions just like a traditional KVM switch – allowing control of up to 64 servers using a single keyboard, monitor, and mouse.
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The Dominion KX II local port has a completely independent access path to the servers. This means a user can access servers locally at the rack – without compromising the number of users that access the rack remotely at the same time.
Can I use a USB keyboard or mouse at the local port?	Yes. Dominion KX II offers both PS/2 and USB keyboard and mouse ports on the local port. Note that the USB ports are USB v1.1, and support keyboards and mice only – not USB devices such as scanners or printers.
Is there an On-Screen Display (OSD) for local, at-the-rack access?	Yes, but Dominion KX II's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, KX II's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at-the-rack.
How do I select between servers while using the local port?	The local port displays the connected servers using the same user interface as the remote client. Connect to a server with a simple click of the mouse.
How do I ensure that only authorized users can access servers from the local port?	<p>Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that:</p> <ul style="list-style-type: none"> • If the Dominion KX II is configured to interact with an external RADIUS, LDAP or Active Directory server, users attempting to access the local port will authenticate against the same server. • If the external authentication servers are unavailable, Dominion KX II fails-over to its own internal authentication database. <p>Dominion KX II has its own standalone authentication, enabling instant, out-of-the-box installation.</p>
If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance?	Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter Secure Gateway management appliance. To be clear, if the name of a server via the Dominion KX II on-screen display is changed, this updates all remote clients and external management servers in real-time.

QUESTION	ANSWER
If I use Dominion KX II's remote administration tools to change the name of a connected server, does that change propagate to the local port OSD as well?	Yes. If the name of a server is changed remotely, or via Raritan's optional CommandCenter Secure Gateway management appliance, this update immediately affects Dominion KX II's on-screen display.
Sometimes I see "shadows" on the local port user interface. Why does that occur?	This shadow/ghosting effect may occur with LCD monitors that have been on for long periods. The LCD properties and the electrical/static charge can produce these effects when the screen is on for a long time.

Power Control

QUESTION	ANSWER
Does Dominion KX II have a dual power option?	All Dominion KX II models come equipped with dual AC inputs and power supplies with automatic fail-over. Should one of the power inputs or power supplies fail, then the KX II will automatically switch to the other.
Does the power supply used by Dominion KX II automatically detect voltage settings?	Yes. Dominion KX II's power supply can be used in AC voltage ranges from 100-240 volts, at 50-60 Hz.
If a power supply or input fails, will I be notified?	The KX II front panel LED will notify the user of a power failure. An entry will also be sent to the Audit Log and displayed on the KX II Remote Client User Interface. If configured by the administrator, then SNMP or Syslog events will be generated.
What type of power control capabilities does Dominion KX II offer?	Raritan's Remote Power Control power strips can be connected to the Dominion KX II to provide power control of the target servers. After a simple one-time configuration step, just right click on the server name to power on, off, or recycle a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.
Does Dominion KX II support servers with multiple power supplies? What if each power supply is connected to a different power strip?	Yes. Dominion KX II can be easily configured to support multiple power supplies connected to multiple power strips. Up to eight (8) power strips can be connected to a KX II device. Four power supplies can be connected per target server to multiple power strips.
Does remote power control require any special server configuration?	Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. See the server user manual for more information.
What type of power strips does Dominion KX II support?	To take advantage of Dominion KX II's integrated power control user interface, and more importantly, integrated security, use Raritan's Remote Power Control (RPC) power strips. RPCs come in many outlet, connector, and amp variations. The D2CIM-PWR must be purchased to connect the RPC to the KX II.

Scalability

QUESTION	ANSWER
<p>How do I connect multiple Dominion KX II devices together into one solution?</p>	<p>Multiple Dominion KX II units do not need to be physically connected together. Instead, each Dominion KX II unit connects to the network, and they automatically work together as a single solution if deployed with Raritan's optional CommandCenter Secure Gateway (CC-SG) management appliance. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database.</p> <p>In addition, CC-SG enables sophisticated server sorting, permissions, and access. If deployment of Raritan's CC-SG management appliance isn't an option, multiple Dominion KX II units still interoperate and scale automatically: The KX II's remote user interface and the Multi-Platform Client will automatically discover Dominion KX II units. Non-discovered Dominion KX II units can be accessed via a user-created profile.</p>
<p>Can I connect an existing analog KVM switch to Dominion KX II?</p>	<p>Yes. Analog KVM switches can be connected to one of Dominion KX II's server ports. Simply use a PS/2 Computer Interface Module (CIM), and attach it to the user ports of the existing analog KVM switch. Please note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information. Raritan's Paragon® and Paragon II analog switches are IP-enabled by the IP-Reach® family of remote access products.</p>

Computer Interface Modules (CIMs)

QUESTION	ANSWER
<p>Can I use Computer Interface Modules (CIMs) from Raritan's analog matrix KVM switch, Paragon, with Dominion KX II?</p>	<p>Yes. Certain Paragon computer interface modules (CIMs) may work with Dominion KX II (please check the Raritan Dominion KX II release notes on the web site for the latest list of certified CIMs).</p> <p>However, because Paragon CIMs cost more than Dominion KX II CIMs (as they incorporate technology for video transmission of up to 1000 feet [300 meters]), it is not generally advisable to purchase Paragon CIMs for use with Dominion KX II. Also note that when connected to Dominion KX II, Paragon CIMs transmit video at a distance of up to 150 feet, the same as Dominion KX II CIMs – not at 1000 feet [300 meters], as they do when connected to Paragon.</p>
<p>Can I use Dominion KX II Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?</p>	<p>No. Dominion KX II computer interface modules (CIMs) transmit video at ranges of 50 to 150 feet (15 – 45 m) and thus do not work with Paragon, which requires CIMs that transmit video at a range of 1000 feet (300 meters). To ensure that all Raritan's customers experience the very best quality video available in the industry – a consistent Raritan characteristic – Dominion Series CIMs do not interoperate with Paragon.</p>

Security

QUESTION	ANSWER														
What kind of encryption does Dominion KX II use?	Dominion KX II uses industry-standard (and extremely secure) 128-bit RC4 or AES encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and Dominion KX II that is not completely secured by encryption.														
Does Dominion KX II support AES encryption as recommended by the US Government's NIST and FIPs standards?	The Dominion KX II utilizes the Advanced Encryption Standard (AES) encryption for added security. AES is a US government approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.														
Does Dominion KX II allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, Dominion KX II does not compromise security – it allows encryption of keyboard, mouse and video data.														
How does Dominion KX II integrate with external authentication servers such as Active Directory®, RADIUS, or LDAP?	Through a very simple configuration, Dominion KX II can be set to forward all authentication requests to an external server such as LDAP, Active Directory, or RADIUS. For each authenticated user, Dominion KX II receives from the authentication server the user group to which that user belongs. Dominion KX II then determines the user's access permissions depending on the user group to which he or she belongs.														
How are usernames and passwords stored?	Should Dominion KX II's internal authentication capabilities be used, all sensitive information such as usernames and passwords are stored in an encrypted format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.														
Does Dominion KX II support strong password?	Yes. The Dominion KX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.														
If the Dominion KX II Encryption Mode is set to Auto, what level of encryption is achieved?	The encryption level that is auto-negotiated is dependent on the browser in use: <table border="1"> <thead> <tr> <th>Browser</th><th>Encryption Level</th></tr> </thead> <tbody> <tr> <td>Internet Explorer 6</td><td>RC4</td></tr> <tr> <td>Internet Explorer 7</td><td>AES-128</td></tr> <tr> <td>Firefox 1.5</td><td>RC4</td></tr> <tr> <td>Firefox 2.0</td><td>RC4</td></tr> <tr> <td>Mozilla 1.7</td><td>RC4</td></tr> <tr> <td>Safari 2.0.4</td><td>AES-128</td></tr> </tbody> </table>	Browser	Encryption Level	Internet Explorer 6	RC4	Internet Explorer 7	AES-128	Firefox 1.5	RC4	Firefox 2.0	RC4	Mozilla 1.7	RC4	Safari 2.0.4	AES-128
Browser	Encryption Level														
Internet Explorer 6	RC4														
Internet Explorer 7	AES-128														
Firefox 1.5	RC4														
Firefox 2.0	RC4														
Mozilla 1.7	RC4														
Safari 2.0.4	AES-128														

Manageability

QUESTION	ANSWER
Can Dominion KX II be remotely managed and configured via Web browser?	<p>Yes. Dominion KX II can be completely configured remotely via Web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed.</p> <p>Besides the initial setting of Dominion KX II's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and Dominion KX II's default IP address, you can even configure the initial settings via Web browser.)</p>
Can I backup and restore Dominion KX II's configuration?	<p>Yes. Dominion KX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.</p> <p>Dominion KX II's backup and restore functionality can be used remotely over the network, or through a Web browser.</p>
What auditing or logging does Dominion KX II offer?	For complete accountability, Dominion KX II logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.
Can Dominion KX II integrate with Syslog?	Yes. In addition to Dominion KX II's own internal logging capabilities, Dominion KX II can send all logged events to a centralized Syslog server.
Can Dominion KX II integrate with SNMP?	Yes. In addition to Dominion KX II's own internal logging capabilities, Dominion KX II can send SNMP traps to SNMP management systems like HP Openview and Raritan's CC-NOC.
Can Dominion KX II's internal clock be synchronized with a timeserver?	Yes. Dominion KX II supports the industry-standard NTP protocol for synchronization with either a corporate timeserver, or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

Miscellaneous

QUESTION	ANSWER
What is Dominion KX II's default IP address?	192.168.0.192
What is Dominion KX II's default username and password?	The KX II's default username and password are admin/raritan [all lower case]. However, for the highest level of security, the KX II forces the administrator to change the Dominion KX II default administrative username and password when the unit is first booted up.
I changed and subsequently forgot Dominion KX II's administrative password; can you retrieve it for me?	KX II contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device.

Troubleshooting

QUESTION	ANSWER
I am logged into the Dominion KX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same Dominion KX II with the second Firefox browser. Is this right?	Yes, this is correct behavior and is the direct result of how browsers and cookies function.
I am logged into the Dominion KX II using Firefox and I attempt to log into another Dominion KX II using another Firefox browser session from the same client. I am logged out of both KX IIs; is this correct behavior?	Yes, to access two different Dominion KX II devices, either close the first session, or use another client PC.
When I'm running a KVM session using Firefox as my browser, and certain dialogs are opened in the Virtual KVM Client (e.g., Connection Properties, Video Settings), it seems to block the Firefox browser (even other Firefox sessions). What can I do?	This is normal behavior; with Firefox, all sessions are associated. Once you close the Virtual KVM Client dialog, Firefox will no longer be blocked.

255-62-4023-00

World Headquarters

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: www.raritan.com

Raritan America

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: www.raritan.com

Asia Pacific Headquarters

Raritan Asia Pacific, Inc.
5F, 121, Lane 235, Pao-Chiao Road,
Hsin Tien 231,
Taipei, Taiwan, ROC
Tel. (886) 2 8919-1333
Fax. (886) 2 8919-1338
Email: sales.asia@raritan.com
Web: raritan-ap.com

Raritan China Offices

Raritan Beijing
No. 35 Financial St, Xicheng District
Room 1035, Block C,
Corporate Square
Beijing 100032, China
Tel: (86) 10-8809-1890
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Shanghai
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai, China
(200030)
Tel. (86) 21 5425-2499
Fax. (86) 21 5425-3992
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Guangzhou
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou (510075), China Raritan
Tel. (86) 20 8755-5581
Fax. (86) 20 8755-5571
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Korea

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel. (82) 2 557-8730
Fax. (82) 2 557-8733
Email: sales.korea@raritan.com
Web: raritan.co.kr

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku, Tokyo 104-0033
Tel. (81) 03-3523-5991
Fax. (81) 03-3523-5992
Email: sales@raritan.co.jp
Web: raritan.co.jp

Raritan Osaka
3rd Floor,
Osaka Kagaku Sen'I Kaikan Bldg.
4-6-8 Kawara-machi, Chuo-ku,
Osaka 541-0048
Tel. (81) 03-3523-5953
Fax. (81) 03-3523-5992
Web: raritan.co.jp

Raritan Australia Offices

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australia
Tel. (61) 3-9866-6887
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan Sydney
PO BOX A386,
Sydney, NSW2000, Australia
Tel: (61) 2-9029-2558
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan India

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli Gurgaon
Rd, Gurgaon 122 002
Haryana, India
Tel. (91) 124 410-7881
Fax. (91) 124 410-7880
Email: enquiry.india@raritan.com
Web: raritan.co.in

Raritan Taiwan

5F, 121, Lane 235, Pao-Chiao Road
Hsin-Tien City
Taipei Hsien, Taiwan, ROC
Tel. (886) 2 8919-1333
Fax. (886) 2 8919-1338
Email: sales.taiwan@raritan.com
Web: raritan.com.tw

Raritan Singapore

350 Orchard Road
#11-08, Suite 21, Shaw House
Singapore 238868
Tel: (65) 6725 9871
Fax : (65) 6725 9872
Email: sales.ap@raritan.com
Web: raritan-ap.com

European Headquarters

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax. (31) 10-284-4049
Email: sales.europe@raritan.com
Web: www.raritan.fr
www.raritan.de

Raritan France

120 Rue Jean Jaures
92300 Levallois-Perret, France
Tel. (33) 14-756-2039
Fax. (33) 14-756-2061
Email: sales.france@raritan.com
Web: www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen, Germany
Tel. (49) 201-747-98-0
Fax. (49) 201-747-98-50
Email: sales.germany@raritan.com
Web: www.raritan.de

Raritan Italia

Via dei Piatti 4
20123 Milan
Italy
Tel. (39) 02-454-76813
Fax. (39) 02-861-749
Email: sales.italy@raritan.com
Web: raritan.it
www.raritan.info

Raritan Canada

Raritan Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Canada
Tel. 1-905-949-3650
Email: sales.canada@raritan.com
Web: raritan.ca

Raritan U.K.

9th Floor, 12-20 Camomile St
London EC3A 7EX, United Kingdom
Tel. (44) (0)20-7614-7700
Email: sales.uk@raritan.com
Web: raritan.co.uk